PCB Hardware Trojans: Attack Modes and Detection Strategies

Matthew McGuire, Umit Ogras, and Sule Ozev
School of Electrical, Computer and Energy Engineering
Arizona State University

Abstract—Prior work on hardware trojans has largely focused on the analysis and detection of implanted trojans in integrated circuits. While a large amount of effort has been put towards the classification and detection of IC-level hardware trojans, comparatively little effort has been expended on the analysis of system or module level attack opportunities. Research is needed on the potential of hardware trojans, even if the design itself is trusted. In this paper, we focus on malicious hardware attacks on printed circuit boards, and assume that the board design is the only trusted part of the final product. We discuss various attack models and propose potential solutions.

I. INTRODUCTION

There has been significant attention in recent years on the security vulnerabilities of integrated circuits (ICs) in the form of hardware trojans, side channel attacks, process and layout modifications [1][2][3]. Specifically, hardware trojans can be inserted into the integrated circuit at any point in the development or production cycle to trigger unintended or malicious operation. Examples of hardware trojans and classification schemes for integrated circuit level hardware trojans are presented in the literature [1][2].

While a large amount of effort has been put towards the classification and detection of integrated circuit hardware trojans, comparatively little effort has been expended on the analysis of system or module level attack opportunities. Unfortunately, printed circuit board (PCB) manufacturing is similarly generalized and open to malicious attacks with the same effectiveness as integrated circuit attacks. The width and spacing of board traces can be changed, modifying the delay and crosstalk parameters and causing parametric failures at production time or in the field [4]. Additionally, traces can be modified to trigger electromigratory failures which may not be detectable through parametric means at production time. Finally, passive components can be modified in functionality or value, leading to malfunction under special operating conditions.

This paper focuses on previously unexplored trojan attack vectors on PCBs and discusses potential solutions. We provide examples of hardware modifications that can induce failure in manufactured devices including an in-depth analysis of a specific kind of malicious attack that is potent in terms of inducing in-field failures but cannot be detected through any of the previously proposed methodologies. We then propose potential solutions for the detection of such trojans and safeguards for these previously unexplored trojans. Finally, we demonstrate these techniques on a PCB design for a wearable sensor and show that the proposed solutions do not add much hardware or test time overhead.

II. RELATED WORK

Trojan detection schemes typically revolve around intentional activation and detection through operational tests of side-channel signals [1][2]. While a large amount of effort has been put towards the classification and detection of integrated circuit hardware trojans, comparatively little effort has been expended on the analysis of system or module level attack opportunities. The PCI-Express device specification defines an implementation of boundary scan for compliant devices and can be used to ensure authenticity and reliability of any attached compliant devices [5]. Additionally, several important features can be implemented in the device’s microprocessor or microcontroller units to provide adequate protection against counterfeit and malicious attacks. First, physically unclonable functions [6] can be used to safeguard against counterfeit integrated circuits by providing a unique but deterministic signature derived during manufacture at a specific fabrication plant. Second, the integrated circuit should provide for JTAG boundary-scan testing to ensure the reliability of the board-level interconnects as mentioned previously. The external interface to this JTAG implementation should be able to be permanently disabled through a hardware fuse or other permanent means to reduce the opportunity for attack in the field after deployment. Finally, all firmware and software for the devices should be flashed once received in a secure test location and not during manufacture to eliminate the possibility of software trojans and tampering.

Various methods that are used in the detection of hardware trojans in integrated circuits such as small delay defect and transition fault testing can also be utilized at the system or module level through application in JTAG boundary scan testing [7],[8]. These methods are useful for sensitive data nets which may not be able to be tested with probe pads or in-circuit test systems. Boundary scan testing, as a particular example, can be used to great effect to determine whether or not a trace between two boundary scan enabled integrated circuits has an open circuit fault. If these open circuit faults are small enough, they may not be apparent in the use of the device with high-speed signals due to their similarity to a distributed element capacitive gap filter. However, slow speed or DC testing would illuminate the fault.

A recent study presents examples of attacks at the PCB level [4]. The authors present a high frequency PCB design where an attacker modifies the inter-trace spacing of internal board traces as well as the individual trace width and thickness. Additionally, the dielectric permittivity of the board material is changed to model aging effects. They show an increase in interference and propagation delay that may induce failures. The authors propose to detect these modifications through delay analysis of the traces. Additionally, this form of attack can be detected through careful X-ray inspection of the board after manufacture to look for anomalies if additional testing time permits.

This paper will focus on the attack modes that are not
previously explored in the literature. The methodologies and results in this paper will be based on trusted design, untrusted manufacture PCB level attacks that are not detectable by conventional testing practices.

III. ATTACK METHODOLOGY

Several attack vectors should be considered to adequately protect a PCB design from malicious or accidental modifications during manufacturing. Additionally, it is important to secure the manufactured device from tampering in the field. Examples of attack vectors are presented in Table I, separated by the type of information the net or vector would contain. The separation into data sensitive and data insensitive regions allows a “divide-and-conquer” approach to design for test (DFT) that can provide appropriate protection from intentional attack or manufacturing defects by allowing flexibility in testing without allowing unintended access to sensitive data.

<table>
<thead>
<tr>
<th>Data Sensitive</th>
<th>Data Insensitive</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU/MCU to/from Memory</td>
<td>Passive Components</td>
</tr>
<tr>
<td>Inter-CPU/MCU Connections</td>
<td>Clock Traces and Components</td>
</tr>
<tr>
<td>Local System Peripherals</td>
<td>Encrypted Communications</td>
</tr>
<tr>
<td>Unencrypted Communications</td>
<td>Remote Peripheral Devices</td>
</tr>
</tbody>
</table>

These regions can be further described by the type of components they contain. The data insensitive nets contain many of the passive supporting components in any given design. The data sensitive nets contain only the critical active integrated circuits and their data line interconnects.

A. Passive Component Variation Attacks

Many surface mount passive devices used in modern devices are visually similar. Thus, they could be easily substituted for devices with different specification or quality. Large differences between components would generally cause detectable operational failures of the device. However, small changes in critical components could easily go unnoticed by visual or operational inspection yet still lead to long-term reliability failures.

An illustrative example of a potential circuit modification that would lead to premature device failure can be presented using the configuration resistors on a commonly used energy harvesting integrated circuit. The Texas Instruments BQ25504 [9] uses resistors to implement lithium polymer cell or supercapacitor under- and over-voltage protection as well as charging enable and disable levels. Of particular concern is the battery under-voltage protection configuration. While overcharging damage of lithium cells is generally catastrophic, it is shown in [10] that the depth of discharge incurred during a lithium-metal-polymer (LMP) chemistry rechargeable cell discharge cycle has a strong correlation with the lifespan of the cell while not having immediately catastrophic effects. The authors find that, when an LMP cell is discharged to approximately 2.55 V, there are phase transformations that cause severe damage to the cell and greatly reduce its lifespan [10]. This study can be used to modify the under-voltage protection of the energy harvester IC to intentionally shorten the life of the attached storage lithium polymer cell. Suppose, for instance, that the original design uses \( R_{UV1} = 4.12 \, \text{M}\Omega \) and \( R_{UV2} = 5.76 \, \text{M}\Omega \) to implement a 3.0 V under-voltage cutoff level. Under this scenario, changing these values to 4.87 M\( \Omega \) and 4.99 M\( \Omega \) would be sufficient to achieve a 2.5 V discharge threshold, significantly shortening the life of the cell. If the resistors used in the circuit are not marked, or the markings are counterfeited, a visual inspection would not be sufficient to identify these changes.

Most multi-layer ceramic capacitors (MLCC) used in reliable device design are derated by 50% or more. This derating factor applies to the sum of the peak AC ripple voltage added to the polarizing DC voltage [11]. Reducing the voltage rating of MLCCs in devices can reduce their effective capacitance due to the behavior of the dielectric material. Additionally, voltages higher than the capacitor rating can cause punch-through and failure of the capacitors. An attacker could replace a properly specified capacitor in a given design with one of lower rated voltage to effectively reduce the capacitance in the circuit when it is powered while still appearing to be the correct capacity when measured out of the circuit. Additionally, a marginally adequate voltage rating may allow the capacitor to accumulate damage in general use, leading to premature failure of the device. These attack methods for passive devices are just a few examples of what is possible for a determined attacker. The detection section will cover methods to mitigate these styles of attack.

B. Solder Material Attacks

Prior evidence that solder composition could be used as a potential attack vector for compromising the integrity of a design comes from the incidents surrounding failing commercial graphics devices in consumer products in 2006 and 2008 [12][13].

Failing commercial graphics devices in consumer products in 2006 and 2008 provide evidence that solder composition can be used as a potential attack vector to compromise the integrity of a PCB design [12][13]. Documented in the filings, customers reported a significant rise in failures of the graphics devices due to a change from eutectic to high-lead alloy solders in the grid array balls and use of a low glass transition temperature \( (T_g) \) underfill [12][13]. These failures occurred as an unintentional side effect of an effort to alleviate problems with joint fractures caused by physical stress during product test.

As an unintended consequence, specific thermal profiles caused these devices to prematurely fail due to differing expansion rates between the eutectic alloy used on the PCB pads and the high-lead alloy used on the package bumps. This problem was amplified by the low-\( T_g \) underfill not providing adequate support to the solder interface under operating temperature. It has been noted that a low-\( T_g \) underfill material passed all JESD22-A104 temperature cycling tests and that these “passing” devices often had a failure rate of up to 60% [14]. These failures occur as tensile stresses when the device passes through a specific temperature range dependent on the underfill \( T_g \), implying that there is a narrow band of temperature that causes failure due to a rapid change in thermal expansion rate. When this problem was identified, eutectic alloys and high-\( T_g \) underfill were used for all future products. To
alleviate failures of existing devices, equipment manufacturers implemented software updates to thermal profiles in an attempt to avoid this critical temperature range.

While the abovementioned problem was not due to an intentional attack, it also shows that the board can be vulnerable to various hard-to-detect changes in the composition of materials. A determined attacker could easily modify the alloy composition of the solder and the type of underfill used in a manufactured device to induce intermittent failure.

C. Electromigration Based Attacks

An exceptionally potent attack mechanism for PCBs is changing the characteristics of the interconnects and thereby making them more prone to aging effects, specifically electromigration. Perhaps the most well-known analysis of electromigration was performed in [15], where the time dependency of a trace failure is correlated to current density, temperature, and process variables, which is also known as Black’s equation:

$$MTBF = \frac{1}{A J^2 e^{\sigma_j L}}$$

In Black’s equation, $A$ is a fitting constant that must be determined empirically. It is a function of the specific composition of the conductor, insulating substrate or layers, and operating conditions. The current density exponent, $n$ is another fitting parameter that requires empirical determination but was found by Black to be approximately 2. The activation energy of copper, $\phi$, varies depending on many factors. It has been shown to be approximately 1.2 eV in thin film conductors [16].

Black’s equation shows that the mean time to failure is inversely proportional to the square of the current density. Consequently, one can reduce the expected lifetime by increasing the current density of a specific trace or region of a circuit. Since the resistivity of a conductor has a linear relationship to thickness, failure time scales much faster than the increase in resistance of the conductor. To reduce the lifetime of a given conductor by a factor of 10 under identical operating conditions, one only needs to reduce the cross-sectional area of that conductor by a factor of approximately 3. This reduction in the cross-sectional area has the effect of increasing the conductor resistance by a factor of 3 as well. However, the change in the resistance may be nearly undetectable in sample analysis. The phenomenon, known as the Blech effect [17], is used to provide a countermeasure for electromigration-induced failures in the field. For a conductor shorter than a given line length $L$, electromigration failure would not occur below a given critical current density $J_c$. The general form of the Blech equation is given by:

$$(j L)_c = \frac{\Omega (\sigma_{kh} - \sigma_0)}{|Z^*| \epsilon \rho}$$

For copper interconnects, the Blech product, $(j L)_c$, has been reported in the range of 2000 to 10,000 A/cm [18] and the critical length $L$ can be determined using these empirical values from a given current density $J$. For 10 mA of current flowing through a typical trace of 5 mil width and 1 oz/ft$^2$ copper, the Blech length can be calculated to be approximately 9 cm, taking the worst-case 2000 A/cm from the experimental results. This may be longer than some high-speed trace lengths and shows that electromigration may not be an issue for some high-speed board designs. However, there is a linear relationship between the cross-sectional area and this critical length. Reducing the thickness of the traces reduces the cross-sectional area and therefore can lead to the traces becoming vulnerable to electromigration-based attacks. To continue the example, by reducing the cross-sectional area by a factor of 3 as before, this critical length would be reduced to 3 cm thereby exposing a design implementing 9 cm traces to an electromigration weakness.

One model used to further analyze electromigration effects is a high-speed microprocessor to memory interconnect. From the datasheet of a 1.35 V DDR3 DRAM memory package [19], the input capacitance of the data lines can be approximated as 2 pF and the slew rate required for proper rated operation is expected to be 1 V/ns or greater for data and clock lines and 2 V/ns or greater for data strobe lines. Using $I(t) = C \frac{dV(t)}{dt}$, the average current on the data strobe line would be 4 mA. While this is a safe value for 9 cm long traces according to the Blech equation for the unmodified trace presented previously, it should be apparent that by decreasing the cross-sectional area of the trace to a third of the original value, the trace could be exposed to electromigration effects. Once the Blech criterion is met, Black’s equation can predict an approximate MTBF of the trace given accurate empirical data.

Perhaps a more interesting and exploitable interconnect example is one of high-speed serial data such as a PCI-Express interface. PCI-Express version 2.1 device lanes can operate at 5 GT/s with stringent timing and data reliability requirements. Often the trace lengths on these devices are much longer than that of the memory devices in the previous example. From the PCI-Express Base Specification Revision 2.1 [5], the clock period is 200 ps +/- 60 fs and the minimum rise and fall times are specified to 15% of this clock period. Taking 53 ps rise and fall times from the Texas Instruments SN65LVPE501 PCI-Express Conditioner/Redriver datasheet [20], the slew rate is approximately 20 V/ns into 2 pF of gate capacitance with a differential voltage of 0.8 V and differential impedance of 100 Ω. This yields an average current of over 50 mA for the 30 ps rise and fall windows within a 200 ps clock cycle. Given the longer trace lengths of PCI-Express interconnections, the Blech criterion would almost certainly apply to PCI-Express signals with standard 5 mil, 1 oz/ft$^2$ copper trace. Hence, reducing the cross-sectional area of these traces to induce early failure would be an extremely applicable attack vector.

IV. ATTACK DETECTION

It is important that thorough use-case and burn-in testing be performed on the final product before deployment. A large number of simple attacks or defects may be illuminated during high-temperature use-case testing including errors in component selection, intentional hardware trojans that are temperature activated or activated by common routines, lamination and material defects in the PCB, and out-of-tolerance operational behaviors such as battery charge and discharge levels or passive component drifts. However, burn-in testing will be ineffective against well hidden or rare activation trojans and defects. For example, extensive thermal cycling of every produced device and executing all possible input and output permutations is both cost and time prohibitive.
A. Passive Device and Solder Material Attack Detection

During design, passive devices and data insensitive nets should be provided with adequate test points and access for an in-circuit testing system to validate the product before deployment. Any in-circuit testing system used for validation should be able to measure trace impedance and passive component parameters, thereby validating that the layout and passive component selection specified by the designer was correctly implemented. Since these nets contain no compromisable information, having exposed test points and adequate access to the traces and components is not a security concern.

Measurement of ceramic capacitors in the circuit should be made with an applied DC offset. This DC bias is necessary to ensure that the effective capacitance is within specification while accounting for derating effects. This allows detection of attack methods exploiting reduction in the voltage rating of the capacitors as previously mentioned. If possible, applying a DC voltage near the rated maximum of the specified capacitor would make any gross voltage rating reduction apparent by causing rapid failure. However, capacitance measurement with a small applied DC bias should be adequate for determining if an attacker has modified the selected components.

If large, high-performance microcontrollers or microprocessors are used in the device, the type and application of solder and protective underfill can become a critical component in the test process. X-ray fluorescence can be implemented during test to identify the composition of solder alloys used in the assembly process and detect changes implemented in manufacture[21]. Underfill composition modifications may be found during an operational test at elevated temperatures combined with mechanical stress of the device. If possible, designs should use leaded through hole (SIP/DIP), small outline (SOIC/SOP), or flat pack devices (QFP/QFN) for higher reliability than ball grid array (BGA) packages under mechanical forces and to eliminate the need for underfill and associated testing.

B. Electromigration Attack Detection

Intuitively, the reduced thickness will result in an increase in the resistance of the traces. Thus, it can change both the delay through the trace and the crosstalk between traces. Unfortunately, upon further mathematical and experimental analysis, we determine that this is not a viable option for detection of thinned traces. Crosstalk is not affected as the changes in mutual capacitance and inductance cancel out [22],[23]. Propagation delay is also not affected as it depends almost entirely on the relative permittivity of the PCB substrate material rather than the geometry of the traces themselves [24]. This phenomenon is demonstrated in Table II which shows the effect of trace thickness on propagation delay. It can be seen that even a significant change in thickness only has a minuscule effect on overall propagation delay. Thus, this form of attack is very potent and cannot be detected through previously proposed methods, including delay measurements and X-ray inspection.

Due to these factors, a clever detection method must be found and implemented. We observe that the reduction of trace thickness results in a change in mutual inductance and capacitance. While the changes in the mutual capacitance and inductance do not result in a measurable delay difference as mentioned before, it does change the resonant frequency of the traces significantly, making the measurement of this frequency a viable avenue for detection. To measure this effect, one trace is designated as the victim line, and one or two traces are designated as aggressor traces on either side of the victim line under test. This test setup is shown in Figure 1, implemented in Keysight ADS [25], that allows measurement of the resonance frequency of various trace geometries. Resonant frequency measurement can be conducted by inducing a fast (67 ps) step function on the aggressor lines on the near end of the trace and observing the oscillatory behavior on the far end of the victim trace.

V. EXPERIMENTAL RESULTS

A. Test Point Insertion

In order to demonstrate the effect of test point insertion, Figure 2 shows a small section of a circuit design before modification to allow test probe access to all passive nets. The modified design in Figure 3 shows that very little (less than 10% of the active area in this example) extra space is required to provide the 1mm test points necessary for an in-circuit tester with microprobes to adequately examine all components for authenticity.

In Figure 3, the only nets which do not have test points inserted are the data sensitive nets between the two devices U3 and U6. For data sensitive nets, it would be preferable to have a significant amount of restriction on physical access or tampering. These sensitive nets should not have exposed pads or connections and would need to be tested with a JTAG boundary scan implementation which could be permanently disabled before deployment. Test vectors and

---

Table II

<table>
<thead>
<tr>
<th>Trace Thickness</th>
<th>1” T_PD (ps)</th>
<th>3” T_PD (ps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.40 mil</td>
<td>137.53</td>
<td>412.59</td>
</tr>
<tr>
<td>1.167 mil</td>
<td>137.75</td>
<td>413.26</td>
</tr>
<tr>
<td>0.933 mil</td>
<td>137.98</td>
<td>413.96</td>
</tr>
<tr>
<td>0.700 mil</td>
<td>138.23</td>
<td>414.70</td>
</tr>
<tr>
<td>0.467 mil</td>
<td>138.49</td>
<td>415.48</td>
</tr>
<tr>
<td>0.233 mil</td>
<td>138.76</td>
<td>416.30</td>
</tr>
</tbody>
</table>

---

Figure 1. Electromigration test and simulation schematic using Keysight ADS
procedures would need to be developed to determine the continuity of traces and authenticity of the manufactured device [26],[27]. However, the development and implementation of these authentication methods are beyond the scope of this paper. Further, the microcontroller or microprocessor could contain self-authentication run time routines based on these boundary scan tests to ensure that field tampering is detected, even if external JTAG access to the device had been disabled before deployment [26],[2].

B. Detection of Electromigration Induced Attacks

For this test, a unit step signal with a rise time of 67 ps was used to emulate PCI Express or other high-speed digital bus architectures. This signal is applied to two traces equidistant on both sides of the victim trace and these aggressor traces are terminated by a 50 Ω resistance in parallel with 2 pF of capacitance, representing the far side of the trace where it is connected to a second chip. The victim trace is terminated to system ground on the near side and attached to an active probe model of 50 MΩ in parallel with 2 pF on the far side. Note that a single trace aggressor with the step signal can be used but the resultant induced resonance will have a proportionally lower amplitude. The substrate is modeled as a standard 0.062 inch thick 2-layer PCB with a 1.4 mil copper thickness on top and bottom layers. The top layer thickness is reduced to 0.467 mil to simulate the 1/3 thickness reduction that could induce premature electromigration failures. All simulations used a trace separation of 20 mil and a strip length of 3 inches. In the time domain, Figure 4 shows the resonant frequency difference between traces of 1.4 mil thickness and 0.467 mil thickness with a constant width of 5 mil.

To account for manufacturing tolerances and to develop a detection and test characterization system, a Monte Carlo simulation of the three different trace widths was performed. Trace widths of 5 mil, 10 mil, and 20 mil with a width variation of +/- 1 mil [28] were used during simulation of the effects of manufacturing variance. The results of this method show that wider traces, and therefore smaller trace width deviations, result in a more easily separable set of devices to classify as passing or failing during test. Figures 5 and 6 show the results of this test for the 5 mil and 20 mil trace width cases.
traces due to width variations, several traces should be tested to minimize the number of false positives while still maintaining a high detection accuracy. Table III shows the statistical results of the simulations as well as the lower frequency threshold and the number of measured traces required to achieve a detection accuracy larger than 99% while minimizing the number of false positives to less than 2.5%. These results show that implementing wider traces will help differentiate traces that have been attacked and having more than one trace to test for an attack can assist in detection while minimizing the number of false positives due to manufacturing variations.

### Table III

<table>
<thead>
<tr>
<th>Nominal Trace Width</th>
<th>5 mil</th>
<th>10 mil</th>
<th>20 mil</th>
</tr>
</thead>
<tbody>
<tr>
<td>μ of 1.4mil (Hz)</td>
<td>401.9M</td>
<td>421.5M</td>
<td>442.7M</td>
</tr>
<tr>
<td>σ of 1.4mil (Hz)</td>
<td>389.2M</td>
<td>411.2M</td>
<td>434.4M</td>
</tr>
<tr>
<td>μ of 0.467mil (Hz)</td>
<td>5.444M</td>
<td>5.965M</td>
<td>6.182M</td>
</tr>
<tr>
<td>σ of 0.467mil (Hz)</td>
<td>5.965M</td>
<td>6.182M</td>
<td>6.450M</td>
</tr>
<tr>
<td># Set Threshold</td>
<td>391M</td>
<td>415.5M</td>
<td>438.5M</td>
</tr>
<tr>
<td># Traces Required</td>
<td>5</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

If provisions are made in the design, this attack method may be detected, whether by inserted test points and high-impedance I/O pad modes or by special JTAG configurations for the connected IC’s that allow rerouting of traces to unused pads. This detection method requires the testing equipment to be able to measure the incident waveform accurately in the time-domain and compute the resonant frequency after stimulation from an extremely fast step function source. A device such as the Microchip SY58081AU universal gate [29] or the TI SN65LVPE501 PCI-Express redriver [20] in test mode configuration can be used to generate this step function with the required rise time into a 50 Ω or 100 Ω termination, respectively. Many high performance oscilloscopes are capable of the accuracy required to capture the waveforms for data analysis and detection measurements.

### VI. Conclusions

In a globalized supply chain, PCB manufacturing is open to tampering by potential rogue vendors or employees. In order to protect electronic circuits, manufactured boards must be tested with security imperatives in mind. This paper presented several attack modes that can be easily implemented by a rogue vendor or employee. We used a divide-and-conquer approach to present potential solutions for different attack modes, which include modifying passive devices in a functionally undetectable manner, modifying the specifications of active components, and modifying trace parameters to induce early lifetime electromigration-induced failures. We also presented detection mechanisms for passive devices, and data-sensitive and data-insensitive traces. We showed that these attack modes can be effectively detected by small design-for-test modifications to the PCB to enable accurate characterization and by testing the resonant frequency of sensitive PCB traces.

### References


19. Samsung Electronics Co., Ltd. 2Gb Industrial C-die DDR3 SDRAM, 6 2010. Rev. 1.0.

20. Texas Instruments. Dual Channel x1 PCIe Redriver/Equalizer, 5 2012. Rev. SSLSE30A.


28. ALLPCB China. About trace width and tolerance.

29. Microchip Technology Inc. Ultra-Precision CML AnyGate with Internal Input and Output Termination, 1 2014. Rev. 1.0.