How Secure Are Printed Circuit Boards Against Trojan Attacks?

Swaroop Ghosh  
Dept. of CSE  
University of S. Florida  
Tampa, FL 33620, USA  
sghosh@cse.usf.edu

Abhishek Basak  
Dept. of EECS  
Case Western Reserve U.  
Cleveland, OH 44106, USA  
axb594@case.edu

Swarup Bhunia  
Dept. of EECS  
Case Western Reserve U.  
Cleveland, OH 44106, USA  
skb21@case.edu

Abstract—Malicious modification of a design in a foundry or design house, referred to as hardware Trojan attacks, are intended to act as a spy or terrorist-on-chip. While these attacks have emerged as major security concerns for Integrated Circuits (ICs), in this paper, we demonstrate similar vulnerabilities at higher level, in particular for Printed Circuit Boards (PCBs). We note that increasing complexity of modern PCBs and growing reliance on third party entities make Trojan attacks in PCBs highly feasible. We introduce possible attack models and demonstrate instances for hardware Trojan insertion in fabricated PCBs that can either cause malfunction or leak secret information. Our investigation reveals that traditional PCB test methodologies can often be ineffective in detecting these Trojans. We also explore possible protection approaches against such attacks including a Reverse Engineering-based detection approach and a low-overhead preventive design solution.

Index Terms—Printed Circuit Board, PCB Trojan, Reverse-engineering

I. INTRODUCTION

Hardware Trojan attacks at the integrated circuit (IC) level have been studied extensively in recent times [1]. Researchers have analyzed the impact of these attacks and explored possible countermeasures for ICs [9] [10]. However, vulnerability with respect to hardware Trojan attacks at higher levels of system abstraction, e.g. at Printed Circuit Board (PCB) level, have not been reported earlier. Previous studies have covered security of PCBs against piracy and various post-fabrication tampering attacks. JTAG (Joint Test Access Group) and other field programmability features e.g., probe pins, unused sockets and USB have been extensively exploited by hackers to gain access to internal features of the designs [2] as well as snooping of secret key, collection of test responses, and manipulating JTAG test pins [3]. One instance demonstrated that Xbox can be hacked by disabling the Digital Rights Management (DRM) policy using JTAG [4]. We note that modern PCBs are becoming increasingly vulnerable to malicious modification of PCBs during design or fabrication in untrusted design or fabrication facilities unlike the widely reported in-field tampering attacks [2-4], such a vulnerability creates a new class of threat for PCBs.

The emerging business model of PCB design and fabrication that favors extensive outsourcing and integration of untrusted components/entities in the PCB life-cycle to lower manufacturing cost [5], makes hardware Trojan attacks in PCBs highly feasible. A closer look at several major electronic products and their PCB manufacturers reveals that different PCBs are often designed in different countries.

Fig. 1. (a) Taxonomy of various attacks on PCB; (b) General model of PCB level hardware Trojan; (c) A specific example of Trojan affecting the external memory access in PCB. Vulnerabilities in PCB design with respect to Trojan attack: (d) Thicker traces for high frequency signals; (e) Pair of signals for differential signaling; and, (f) Group of traces indicating bus.
Moreover, reliance to third party manufacturing facilities, make the PCB fabrication process untrustworthy and hence, vulnerable to malicious modifications i.e. Trojan insertion. Furthermore, an adversary can be present inside the design house and the PCB design can be tampered with Trojans. Fig. 1(a) shows broad classes of attacks on PCB including possible Trojan attacks. In this paper, for the first time to our knowledge, we analyze the feasibility of such attack; present attack models and instances of hard-to-detect Trojans; and propose possible countermeasures.

PCBs in today’s complex and highly integrated designs contain as many as 20-30 layers with hidden vias and embedded passive components [12] to minimize the PCB form factor. This presents great opportunity for an attacker to deliberately modify the PCB design by tampering the interconnect lines at the internal layers or altering the components. Fig. 1(b) shows a general model of PCB hardware Trojan. Fig. 1(c) illustrates an example where the external memory content is modified by tampering the write enable signal. Similar to its IC counterpart, a PCB Trojan can serve two purposes for an adversary: (1) cause malfunction; or (2) leak secret information. For example, an added capacitor on a signal line can significantly slow down the communication between the components in specific rare scenarios, making the product fail in field. Similarly, a hacker can access the secret content inside the components and alter/corrupt them.

II. THREAT ANALYSIS AND ATTACK MODELS

A. Security Analysis

An attacker can exploit the vulnerabilities, design/test features and test hooks that are available on the board. Some common PCB features that can be exploited by an adversary for understanding a design intent and efficiently mounting a Trojan attack with minimal design modification are as follows.

1) JTAG interface: JTAG is an industry standard to enable board level test and debug. It can be exploited by a hacker to get a clue about the hidden test features or hidden control to access the data and address bus within the chip. For example, hackers can deduce information about the length and properties of the instruction register through JTAG by trial and error. Next, a particular instruction can be executed to gain permission to tamper/feed internal data bus. JTAG can also be used to Reverse Engineer (RE) the board design by deducing the connectivity between components and executing external connectivity instructions.

2) Test pins or probe pads: Typical ICs contain several probe pads and test pins to observe/control important signals for test/debug purposes. A hacker can tap these pins and monitor the interesting signals to gain critical information about the functionality of the design or feed malicious data into the design. Test pins can also be used for RE where a test input can trigger certain data, address and control signals that can help identify the board functionality.

3) Vulnerabilities in PCB design: Fig. 1(d)-1(f) illustrate several additional vulnerabilities as described below.

   a) Distinct properties of special signals: The thickness of clock and data bus provides clues to the hackers about the functionalities of these pins. Similarly, pins tied with identical pull-up/down resistors indicate that they belong to a bus.

   b) Remnant signatures from test/debug: When pins (that are used for test/debug) are accessed through ports, the remnant of soldering provides clue to a hacker about the functionality of these pins. Similarly, an empty socket can be used for hacking purposes.

   c) Miscellaneous hints: Fig. 2(a) lists some additional vulnerabilities. Apart from above component level hooks, a PCB design itself provides lots of information to an adversary in fabrication house that can facilitate powerful Trojan attacks.

B. Attack Models

Trojan attacks in PCB can be divided into two broad classes, as described below.

1) Case I: The board design is trusted: In this model, the attack is mounted in the PCB fabrication house. It is expected that the attacker would change the design in a way that evades post-manufacturing test, but causes functional deviations under certain rare conditions, which are unlikely to be triggered during test.

2) Case II: The board design is not trusted (e.g. outsourced): In this model, the attacker is assumed to be present in the board design or fabrication house. Only the functional and parametric specifications of the board are trusted. The attacker has higher flexibility of maliciously altering the design and/or choosing fake or untrustworthy (and potentially malicious) components. Again, an attacker would try to hide the modifications to avoid detection during functional and parametric testing process.

Note that in both cases, there are two possible objectives of the attacker: 1) malfunction, and/or 2) information leakage. Next, we describe possible Trojan attacks of different forms in a PCB.

   a) Signal trace modifications in the inner PCB layers: For boards with fewer levels where hiding an extra component is difficult, an attacker can change the resistance, capacitance or inductance of the signal traces (self, mutual). For example, signal trace in an internal layer can be made thinner to increase the resistance such that it fails during long hour of operation due to heating. Similarly the metal coupling capacitance, between two traces including traces in the supply planes can be increased (by changing trace dimensions, intertrace distance via slight rerouting and selective dielectric property modification) to trigger coupling induced voltage and delay failures in one of the lines. Leakage resistance paths can also be incorporated in an internal layer trace for intentional voltage degradation. Impedance mismatch between interconnected traces can be introduced to cause malfunction in certain scenarios.

   Modification in an example 4-trace scenario, causing malicious effects on circuit parameters (coupled voltage, delay
failures and voltage degradation), is illustrated in a commercial Arduino Uno Board layout in Fig. 2(c). It involves changing the thickness and inter-trace distances by 2X and rerouting of single trace. Even in a small 2-layer board design like the UNO, these changes are minimal and difficult to detect during test, but can cause undesired functional behavior under certain scenarios. In complex PCB designs with more than 4 layers, these changes would be confined within a small area of an internal layer. Hence, the chances of detection with optical or X-ray based imaging are extremely low. Functional testing is typically not exhaustive and hence these can easily bypass detection. However, in certain rare conditions in field, their effect on circuit parameters can be significant causing system failures.

b) Hidden components: For boards with more than two layers, an adversary can insert extra components in an internal layer to either leak information or conditionally cause malfunctions. Replacing a legitimate IC with Trojan infected IC is another possibility. The tampered IC would be functionally equivalent to the legal IC, however, it may be equipped with capabilities to leak secret information. The leakage can be direct (through unused pins) or indirect (modulating supply voltage or current). Fig. 1(a) summarizes different categories of PCB attacks.

C. PCB Fabrication and Test

The PCB fabrication process consists of steps such as inner layer processing, mass lamination, drilling, copper plating, outer layer processing, solder mask, silk screen, gold finger plating, HASL, routing. The resistors, capacitors and inductors are embedded during the screening stage to reduce the form factor of the PCB [12]. For example, polymer thick film (PTF) resistive paste is screened on the PCB surface to create resistance. Each layer of the PCB is screened with appropriate materials to realize passive components and baked in oven to dry the material. Finally, the layers are bonded together. After fabrication, traditional validation of PCB involves finding the shorts and opens using electrical test, optical inspection and stress test. Once the ICs are integrated on the PCB, boundary scan test using JTAG combined with built-in test pattern generators are employed for stuck-at and crosstalk testing [11] of interconnects. Note that the existing board testing methodology is not tailored for Trojan sensitization and detection. However, this infrastructure could be expanded to cover the Trojans.

III. ATTACK INSTANCES

A. Design House is Trusted

This scenario arises when the PCB is designed by a trusted designer and outsourced for fabrication. During the manufacturing process, malicious modifications can be intelligently inserted by an adversary, such that the final design structurally matches the original one (no additional components, logic, traces), but produces undesired functionality under certain conditions. The small alterations can be confined in the internal layers of a multi-layer PCB. Hence, chances of detection with visual inspection, optical imaging and X-ray based imaging techniques are low. Besides, exhaustive functional testing is typically impossible with large number of test nodes. Therefore, the malicious functions are very likely not triggered during the in-circuit and boundary scan based functional testing [6]. Usually modifications can be made in the existing traces to increase the mutual coupling capacitance, characteristic impedance, or loop inductance by changes in internal layer routing and small leakage path insertion. Additional components with ultra-low area and power requirements can also be inserted in the internal layers.

We present two Trojan examples in this class. The first case considers a multi-layer PCB (10 cm length) with possible application in a high-speed communication and video...
streaming systems. It has a common scenario of two High Frequency (HF) PCB traces in an internal layer running parallel to each other. Typically, HF traces are routed in the internal layer shielded by power and ground planes to avoid interference (Fig. 3(a)). However, it significantly complicates the internal layer testing and debug procedure and provides an opportunity to the attacker. The dimensions of the traces are designed optimally to carry normal HF signals i.e., 1 oz. copper trace with width and thickness of 6 mils and 1.4 mils, respectively [7]. The dielectric is FR-4 with a relative permittivity of 4.5. The inter-trace distance is chosen to be 30-40 mils to avoid the negative effects of mutual inductive and capacitive coupling. These HF traces are modeled by lumped parametric form [7]. Functional simulation shows a maximum coupled near and far end voltage of ~300 mV p-p on one of the traces, with the other trace swept with pulse voltages of 3V p-p at 10−500 MHz with a 50% duty cycle. The maximum propagation delay for the pulse across the active trace is ~0.4 ns.

With the simulation setup described above, we observe the effects of various trace level modifications during fabrication. The inter-trace distance in the internal layers is reduced by 2X, widths of both the wires are increased by 2X and the thickness is increased by 1.5X. These are minimal changes in a small target region of an internal layer, rendering them mostly undetectable during structural testing. The dielectric permittivity of the insulator between the traces is increased to 5.5 in order to model moisture retention in certain insulating areas, impurity addition to epoxy base [8] and hence, the aging effect. Accelerated aging tests have a low probability of detecting this as the permittivity is selectively altered by an adversary in a small area. However, the effect of these changes on associated circuit parameters can be significant. At 220 MHz, the near end peak-to-peak voltage in trace-2 is ~1.4 V for an input pulse voltage of 3V p-p in trace-1 (Fig. 3(b)). This is an extraneous interference and may cause unexpected behavior in terms of erroneous circuit activation or feedback. The propagation delay increases by 2X, beyond 1ns (Fig. 3(c)) which can induce functional failures for higher switching frequencies and greater trace lengths. From an attacker’s perspective, inserting a small leakage path (2X the trace resistances) to ground can drain away the signal, resulting in a degraded, distorted waveform at the far end of trace-1 (Fig. 3(d)) and hence malfunction in the connecting circuits. This can easily evade detection by conventional PCB testing which is not exhaustive due to prohibitive cost and time-to-market.

The effect of coupling is more prominent when multiple HF traces, over different planes are intentionally routed intelligently to increase mutual coupling. This can be achieved by: (a) bringing the in-plane neighboring traces closer, and (b) increasing widths and thicknesses of the lines. These selective minute alterations are highly likely to pass structural and functional testing. However, the effect of these changes on the circuit performance could be significant as shown in Fig. 3(e)-3(f). The coupled voltages at the near and far end of victim trace-1 is 3.1 V p-p and 1.3 V p-p, respectively (Fig. 3(e)) with in-phase rising/falling transition on the adjacent 3 traces (1 in-plane, 1 above and 1 below). This is 3-4 X greater than the case when active traces are switching in opposite directions. This interference would certainly result in failures in terms of erroneous activation, feedback and performance. The voltage profile at the far end of trace-1 with the others inactive, show some distortion and an unexpected behavior (Fig. 3(f)). Higher number of neighboring traces, and greater trace lengths significantly
affect the propagation delay and causes delay failures at high switching speeds. Extraneous coupled voltages in traces 3 and 4 are illustrated in Fig. 3(f) as well. It can be noted from above results that detecting these Trojans are extremely hard since it is sensitized under very rare specific conditions. In the multi-wire scenario, the degraded performance is prominent only in 2 out of 8 possible combinations of transition polarity (i.e., all rising/falling pulses) in the 3 neighboring traces. The frequency of operation and the input vector patterns serve as two example conditional triggers for these Trojans, inserted by selective trace property and routing alterations during PCB fabrication.

**B. Design House is Untrusted**

In this attack model, both PCB design and fabrication are done in untrusted facilities, thus, increasing the possibility of Trojan attacks. The board specifications generated by the system designer is trusted. Post manufacturing testing is done by the system designer to ensure the board performance and functionality. Hence, along with the possibilities of trace level alterations, an attacker can also leverage the opportunity to modify the design structurally and/or insert additional components that would be activated upon certain trigger conditions. The design alterations would be hidden intelligently (e.g., physically or by rare input conditions) to evade detection during post fabrication structural and functional testing. A simple example of this attack model is illustrated in Fig. 4, where a fan controller adjusts the speed of a 12 V DC brushless fan based on the input received from a temperature sensor. The sensor provides 0-5V (depending on the current temperature) which is digitized by an ADC and sent to a microcontroller that controls the speed of the fan through linear regulation of the fan input voltage.

With minor structural modification, an attacker can maliciously tamper with the functionality of the circuit (Fig. 4(a)). In this case, the Trojan prevents the microcontroller from obtaining an accurate temperature. It includes a resistance, a capacitor and a PMOS transistor. The capacitor is charged using the output from a voltage regulator (LM317) connected to the fan. The time needed to activate the Trojan (i.e., the trigger condition) can be adjusted by manipulating the resistance and capacitance values. The trigger de-activates the PMOS transistor inserted between the temperature sensor and the ADC, effectively disabling the connection. Hence, the microcontroller receives a null input that is interpreted as a very low temperature and the fan speed is reduced significantly. With a large value of time constant, this design alteration has a high probability of evading functional testing. A 2-layer PCB schematic of the fan-controller (pre-fabrication) is shown in Fig. 4(b). A fabricated PCB board to demonstrate the triggering and payload of the Trojan, is shown in Fig. 4(c).

From the above discussion, it is obvious that achieving these minor structural modifications in such a scenario is easy due to outsourcing of both design and fabrication. Since system integrator only possesses information about the major PCB components (constituent ICs) and functional specifications, such small alternations can go undetected. From the attacker’s perspective, a multi-layered PCB is more attractive because it provides increased opportunities to hide the design changes. In addition to the structural changes, an adversary in the foundry can perform layout modifications to deliberately insert trace level Trojans, which are difficult to identify by functional tests.

**IV. Possible Countermeasures**

**A. Hardware Trojan Detection in PCB**

We propose non-invasive RE and multi-parameter side-channel analysis to detect the embedded Trojans. First, the Trojans are categorized by their nature e.g., Trojans that induce: (a) parametric failures, such as unacceptable delay and leakage ($T_{par}$); (b) large static power ($T_{pwr}$); and (c) functional failures ($T_{fn}$). Trojans in each category are treated differently for detection. Next, a criticality analysis is performed to isolate the vulnerable nodes. This step is conducted to identify the critical signals from design specification e.g., clock, control signals, data and address bus. The PCB layout information is captured in the analysis to identify the potential Trojans (i.e., the longest trace that runs in parallel with the victim signal). For analysis we assume that, (a) intended PCB design is available to the validation engineer; (b) a single Trojan is inserted at a time; (c) Trojan injection is limited to neighboring traces; and, (d) tampering do not involve change in the signal routing.

Test pattern generation for Trojan detection can leverage on the principles of conventional testing. The PCB layout and criticality analysis generate a list of possible triggers/payloads and their locations. Test patterns are generated to sensitize the trigger conditions of each Trojan and observe its effect. The process continues till all the Trojans are identified.
in the list are exhausted. Side channel analysis such as delay, frequency, static leakage and dynamic current can also be administered to sensitize Trojans of other types. Side-channel analysis, however, would require a set of golden PCBs. The Trojan coverage and the test patterns are output of the proposed methodology (Fig. 5(a)). The test patterns obtained above are applied to both extracted parasitic model and actual PCB, and, their responses are compared to detect Trojans. Fig. 5(b) illustrates this methodology for capacitive Trojans through an example where net n3 is identified as the target signal from node criticality analysis. Therefore, the Trojan list would contain \{c_1, c_5, c_6\}. For this example, test pattern will target to toggle nets n1, n3 and n5 in association with n3 to sensitize the Trojans for detection. Note that c2 is excluded from the list due to shorter track segment of n2 in parallel with n3.

**B. Preventive Countermeasures through Hardening**

We propose following proactive techniques to protect against Trojan attacks in PCBs:

1) **Secure Interfaces:** Conventional JTAG cannot prevent unauthorized access and therefore it can be exposed for tampering. We update the security features inside JTAG so that the access to instruction and data registers is restricted until a code/password is fed to unlock the TAP controller. Fig. 5(c) shows the JTAG structure containing TAP controller that provides access to the instruction and data register (device registers, ID register and bypass register) based on TMS and TCK. The modified TAP controller (Fig. 5(d)) includes newly added states (S0-S3) that look for a certain security key. In order to allow legitimate access (for installing upgrades and patches), the secure JTAG can be unlocked by feeding the correct keyword (0011111 in this case). However, in the event of wrong keyword, the controller will go to a lock state (S4) where it will disconnect the TDI and TDO by feeding a fixed value to TDO. Note that once the TAP goes to the lock state it cannot be reset back to factory state preventing the possibility of a trial-and-error method by the hacker.

2) **Secure PCB:** Conventionally designed PCB traces can be reverse-engineered to discover the board design. We propose an approach to address this challenge through interconnect obfuscation. Fig. 5(e) shows one possible approach to obfuscate the interconnects by introducing dummy ICs that serves three purposes: (a) it scrambles the traces based on a scrambling function implemented in the dummy logic. The dummy device is RE-resistant due to presence of secure JTAG that prevents access to internal design without proper authentication; (b) it provides dummy outputs that are mixed with real traces to confuse the hacker. The dummy traces are driven by random logic and counters to obfuscate the data, address and clock signals. Furthermore, the dummy traces are drawn in the same way as the real data and clock signals to obfuscate the real signals; and, (c) it implements secure JTAG therefore the access to real chips is also secured even if they implement unsecured JTAG. In order to RE the real chips, the hacker needs to unlock the JTAG of two dummy chips (D0 and D1) each of them may have different security keywords. RE through JTAG could be deterred further by incorporating the security states in the TAP controller of the real chips as well.

**V. CONCLUSION AND FUTURE DIRECTIONS**

We have analyzed the threat of hardware Trojan attacks in PCBs. We have shown that clever localized modifications in PCB during design or fabrication can evade conventional structural and functional testing. They can lead to malicious and often catastrophic outcomes during field operation. We have also presented two possible countermeasures through judicious trust validation and low-cost design approaches. With growing complexity of multi-layer PCBs including hidden vias and increasing reliance on third party resources, more complex Trojan attacks would become feasible. Due to wide-spread use of PCBs, their vulnerability to Trojan attacks poses major concerns in trust and security of electronic products. Untrusted PCBs can enable highly sophisticated and powerful attacks such as unauthorized access to a system or wirelessly transmitting secret data. Future work would
include analysis of more complex attacks and exploration of Trojan attacks beyond PCB level.

VI. ACKNOWLEDGMENTS

The work is supported in part by National Science Foundation grants CNS-1054744 and DUE-1245756.

REFERENCES


Swaroop Ghosh (M’08 –SM’13) is an assistant professor at University of South Florida. He received his Ph.D. from Purdue University. He was a senior research and development engineer in Advanced Design, Intel Corporation. His research interests include energy-efficient, robust and secure circuits and system design and, digital testing for nanometer technologies.

Abhishek Basak (S’11) received his B.E. (Hons.) from Jadavpur University, Kolkata, India in 2010 and is currently pursuing his Ph.D. degree in Computer Engineering at Case Western Reserve University, Ohio. He research interests lie in hardware security and trust as well as biomedical system design for point-of-care health monitoring.

Swarup Bhunia (M’05 –SM’09) is T. and A. Schroeder associate professor of electrical engineering and computer science at Case Western Reserve University, Ohio. His research interests include low-power and robust design, hardware security and implantable electronics. He received his PhD in electrical engineering from Purdue University.