Parasitic Circus: On the Feasibility of Golden-free PCB Verification

Maryam Saadat Safa, Patrick Schaumont and Shahin Tajik
Worcester Polytechnic Institute, Worcester, MA, USA
{msafa, pschaumont, stajik}@wpi.edu

***Abstract*— Printed circuit boards (PCBs) are an integral part of electronic systems. Hence, verifying their physical integrity in the presence of supply chain attacks (e.g., tampering and counterfeiting) is of utmost importance. While traditional methods depend on a physical golden sample for signature comparison, accessing such a sample for golden signature extraction is often impractical in real-world scenarios. In this work, we assess the feasibility of replacing the *physical* golden sample with a simulated golden signature obtained from the PCB design files. By performing extensive simulation and measurements on an in-house designed PCB, we demonstrate how the parasitic impedance of the PCB components plays a major role in reaching a successful verification. Based on the obtained results and using statistical metrics, we show that we can mitigate the discrepancy between collected signatures from simulation and measurements.**

***Keywords*— Hardware Trojans, PCB Verification, Power Delivery Network, Scattering Parameters, Tamper Detection.**

I. Introduction

Printed Circuit Boards (PCBs) play a crucial role in electronic systems. Given the globalization of the PCB manufacturing and assembly process, they are susceptible to various attacks, rendering them potentially insecure. Conventional verification methods rely on the existence of a physical golden sample for signature comparisons [1], [2]. While these methods are both precise and efficient, similar to other physical verification methods, the dependence on golden samples for comparison poses a significant challenge. Acquiring these golden samples is notably difficult as a trustworthy PCB assembly factory should exist to manufacture them. Naturally, such a condition might not be met in real-world scenarios, and only the design files of the system (e.g., PCB netlist, bill of material, and IC package specifications) are accessible to the verifier. Recent studies have tried to remove the physical golden sample necessity in tamper detection, but these methods are limited to the PCB's circuit [3] and cannot detect physical changes like adding an extra via or altering PCB materials.

II. Background

The real-world PCB components contain parasitics making them behave differently from their ideal models. For instance, in addition to the capacitive behavior, capacitors manifest resistive and inductive characteristics as well, commonly referred to as Equivalent Series Resistance (ESR) and Equivalent Series Inductance (ESL), respectively. The introduction of components, such as non-ideal capacitors, as illustrated in Fig. 1(a), is modeled by incorporating an RLC branch into the circuit model. By adding a component to the Power Delivery Network (PDN), the equivalent capacitance and inductance of the system change, and consequently, the resonance frequency also shifts in the frequency domain as shown in Fig. 1(c) and (d). Accurate estimation of parasitic impedance is essential in our study, as we analyze the impact of tampering (e.g., addition or removal of components).

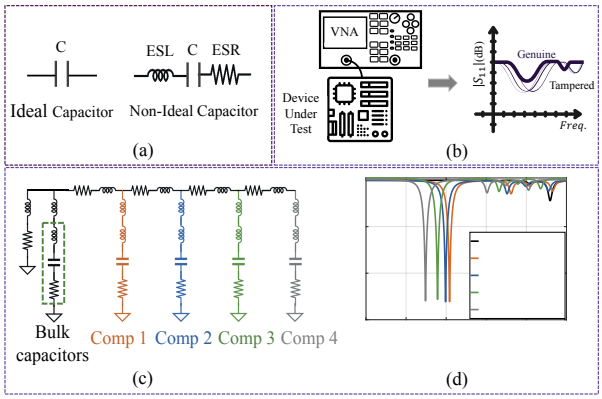

Fig. 1. (a) Impedance profile of an ideal and non-ideal capacitor. (b) Hardware signature extraction based on reflection method.(c) PDN circuit model of the PCB. (d) The simulated $|S_{11}|$ displays the impedance contribution of each component.

III. Methodology

In this paper, we extend the impedance-based PCB verification method [1] so that it leverages PCB design files to generate an estimated golden signature. We utilize scattering parameter analysis, especially the reflection response denoted as $|S_{11}|$, which can be measured using a Vector Network Analyzer (VNA), as illustrated in Fig. 1(b). In the first phase of the verification process, a trusted PCB design file is used to generate the golden signature. This process involves importing the PCB design files and extracting the PCB's electrical characteristics by deploying the simulated $|S_{11}|$ profile, which is an alternative representation of the system's impedance. Thereafter, in the second phase, the verifier conducts $|S_{11}|$ measurements on the PDNs of a population of PCB samples. Then, the Dynamic Time Warping (DTW) metric [4] is used to compute the distance between the golden simulated signature and each of the collected measured signatures. The evaluation criteria are set based on the DTW score. If the DTW score is below a predefined threshold, the test will be passed, and the sample will be verified as genuine; otherwise, the test fails, and the sample will be considered dissimilar. Note that main

979-8-3503-4859-0/DATE24/© 2024 EDAA

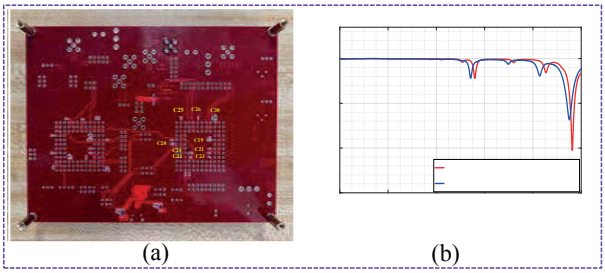

Fig. 2. (a) Backside of the board under test. Capacitors integrated into the PDN are highlighted. (b) Simulated signature of $|S_{11}|$ extracted from ANSYS SIwave and measured $|S_{11}|$ of the bare board.

advantage of DTW is its ability to eliminate consistent shifts caused by process variation.

Validation: We validated our approach using an in-house designed PCB with three distinct PDNs. However, we focus on the 1V8 PDN. We employed ANSYS SIwave 2023 R2, which is a powerful 2.5D electromagnetic simulation tool. To emulate PCB-level tamper events, we added five sets of decoupling capacitors to the PDN under test at each trial, see Fig. 2(a). The addition of capacitors to the PDN causes a change in the PDN's impedance, thereby affecting the $|S_{11}|$. Our findings highlight the critical role of the parasitic impedance of PCB components, such as ESR and ESL, in ensuring successful verification. It is essential for the verifier to determine a threshold in accordance with the application and ESR/ESL values. To detect more advanced tampering activities, a higher degree of precision in parasitic impedance values is requisite.

IV. Results

The procedure began with simulating a bare board layout in the simulation software, which lacked any components. This simulation helped in acquiring the $|S_{11}|$ signature, as shown in Fig. 2(b), where the simulated and measurement signatures closely align. A notable 17.2 MHz discrepancy is attributed to substrate impurities, given the absence of board components. Following this, capacitors were added to the PCB's PDN at each trial. The results are discussed through two case studies.

1) *Case Study 1: Addition or Removal of Components*

To generate the simulated golden signature for each trial, the verifier sets the expected values for parasitic impedance of the PCB's component. As illustrated in Table. 1, the first row represents the reference signature obtained from the simulation data and the first column as the measured signatures corresponding to each of the experiments, the values in the diagonal cells represent the DTW distances between the simulation and measurement data of each experiment. As it can be observed the simulated and measured $|S_{11}|$ signatures of identical configurations exhibit lower DTW distances compared to cases, where the simulated configuration differs from the physical sample configuration.

2) *Case Study 2: Replacing Parts with Counterfeit Ones*

In this case study, we assess the feasibility of detecting a component that has been replaced with a counterfeit part. The assumption here is that the counterfeit part has a significant parasitic impedance deviation. Since we did not have access to counterfeit components, we edited instead the ESL and ESR values in our simulations. We chose deviations in the order of 10 and 1.3 for our ESL and ESR values. Such factors were obtained by averaging the existing ESL and ESR values of similar components from various vendors mentioned in their datasheets. As can be observed in Table. 2, the measured and simulated signatures exhibit substantial disparities to the point where the DTW distance between them becomes very large compared to the distances of the previous case study, where no components were added or removed. This confirms that replacing components with fake parts could be detected if the fake parts have a different parasitic behavior.

Table 1. Case Study 1: DTW distances using approximate values of ESR and ESL. (S) indicates simulation, (M) indicates measurement.

Reference ⇒ *Test* ⇓	Bare Board (S)	2 Caps (S)	3 Caps (S)	5 Caps (S)	7 Caps (S)	9 Caps (S)
Bare Board (M)	**189**	1247	1250	1316	1295	1264
2 Caps (M)	1291	**23.8**	33	1316	1270	1239
3 Caps (M)	1283	41.8	**30**	1329	1286	1261
5 Caps (M)	1308	1224	1227	**21.3**	715	1211
7 Caps (M)	1305	1232	1235	60.2	**170**	1210
9 Caps (M)	1205	1247	1251	1331	1263	**212**

Table 2. Case Study 2: DTW distances using deviating values of ESL and ESR showing significantly larger DTW distances than the diagonal cell values in the Table. 1.

Sim vs Meas	2 Caps	3 Caps	5 Caps	7 Caps	9 Caps
DTW Distances	1100	1095	1205	1127	856

Our results demonstrate that mutual coupling between PDNs enables the detection of impedance changes in one PDN using another. For instance, adding a third capacitor in the third trial, not connected to the tested PDN, altered the $|S_{11}|$ parameter and affected the DTW distances. This is particularly useful when access is limited to a single PDN, yet it allows for identifying tampering in other PDNs.

V. Conclusion

In this paper, we explored the feasibility of using simulated golden signatures as a substitute for the physical ones for verification purposes. Our results demonstrate that, with accurately estimated parasitic impedance values of PCB components, it is feasible to rely on a simulated signature as a golden reference.

References

[1] T. Mosavirik *et al.*, "Scatterverif: Verification of electronic boards using reflection response of power distribution network," *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, vol. 18, no. 4, pp. 1–24, 2022.

[2] M. S. Safa *et al.*, "Counterfeit chip detection using scattering parameter analysis," in *2023 26th International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS)*, IEEE, 2023.

[3] A. Bhattacharyay *et al.*, "VIPR-PCB: a machine learning based golden-free PCB assurance framework," in *Proceedings of the 59th ACM/IEEE Design Automation Conference*, pp. 793–798, 2022.

[4] T. K. Vintsyuk, "Speech discrimination by dynamic programming," *Cybernetics*, vol. 4, no. 1, pp. 52–57, 1968.