Title: On the Feasibility of Golden-free PCB Verification in the Zero-trust Model

Abstract: 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. Similar to the Zero-trust concept, which emphasizes "never trust, always verify," there is a focus on rigorous verification in PCB assessments. Every PCB must undergo verification against a golden signature to confirm its authenticity. The conventional verification methods rely on the existence of a physical golden sample for signature comparisons. However, placing trust in the physical golden sample is not a secure option and obtaining these golden samples poses a significant challenge, requiring the presence of a reliable PCB assembly factory for their production. In practical situations, this prerequisite may not always be fulfilled. Often, verifiers may only have access to the system's design files, such as the PCB netlist, bill of materials, and IC package specifications. Therefore, it is crucial to develop a detection technique that does not rely on a physical golden sample and solely depends on the design file.

In this talk, we investigate a generic method for leveraging PCB design files to generate an estimated golden signature, which is then compared to the measured signature of untrusted boards. In the first phase, a trusted PCB design file is employed to generate the golden sample signature. The process involves importing and extracting the electrical characteristics of the PCB from its design file, followed by exporting the S-parameter ($|S_{11}|$) signature of the PCB using simulation software. In the second phase, the verifier performs $|S_{11}|$ measurements using a vector network analyzer (VNA) on the power delivery networks (PDNs) of a population of PCB samples. Afterward, the verifier will apply a similarity measure called Dynamic Time Warping (DTW) metric on the generated simulated golden signature and each of collected measured signatures. If the DTW score is below a predefined threshold, the test will be passed, and the sample is verified as genuine, otherwise, the test fails, and the sample will be considered dissimilar.

To validate this approach, we utilized an in-house designed PCB which contains three distinct and isolated PDNs. The process involves importing and extracting the electrical characteristics of the PCB from its design file, followed by exporting the S-parameter signature using ANSYS SIwave 2023 R2, which is a powerful 2.5D electromagnetic (EM) simulation tool. To emulate PCB tampering, decoupling capacitors of varying capacitances are added into the PDN under test on the board, conducted over six trials. The addition of capacitors to the PDN causes a change in the PDN's impedance, thereby affecting the $|S_{11}|$. Finally, we compare the trusted simulated data to the measured signature derived from the same physical layout using DTW.

We demonstrate that the parasitic impedance of the PCB components including Equivalent Series Resistance (ESR) and Equivalent Series Inductance (ESL) is pivotal in achieving successful verification. The verifier should set a threshold during the design phase of the PCB. Based on the applications where the PCB will be implemented, the verifier has the discretion to determine different tolerances for the parasitic of components. To detect more advanced tampering, a higher degree of precision in parasitic impedance values is requisite. Having the approximate values of parasitic inductance and resistance in simulation tools enables more accurate predictions of the impedance behavior and the discrepancy between collected signatures from simulation and measurements would be minimum. The method is discussed through two case studies.

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.

Table.1: Case Study 1: DTW distances using approximate values of parasitic impedance values showing the impact of adding or removing components. Diagonal cell values represent lower DTW distances, illustrating golden detection with no components added or removed.

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

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. 2: DTW distances using deviating values of ESL and ESR to emulate the replacement genuine parts with counterfeit ones 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 Distance	1100	1095	1205	1127	856

We also show that the mutual coupling between PDNs allows us to detect alterations in the impedance within one PDN by leveraging another PDN. This becomes especially valuable in situations where access is typically limited to a single PDN, yet we maintain the ability to identify tampers associated with other PDNs.

Biography:

Maryam Saadat Safa received the M.Sc. degree in Electrical Engineering from Iran University of Science and Technology (IUST), Tehran, Iran in 2018, where she was a research assistant at the antenna and microwave research laboratory. Since 2022, she has been pursuing the Ph.D. degree in Electrical Engineering at Worcester Polytechnic Institute (WPI), Worcester, MA, USA, at the Vernam applied cryptography and secure embedded systems laboratory (Chips Center). Her research interests include hardware security, physical characterization of electronic systems, and signal/power integrity.