Active Protection against PCB Physical Tampering

Steven Paley
Case Western Reserve University
Cleveland, OH, USA
sjp78@case.edu

Tamzidul Hoque, Swarup Bhunia
University of Florida
Gainesville, FL, USA
{thoque,swarup}@ufl.edu

***Abstract*—A printed circuit board (PCB) acts as the backbone of any electronic system hardware by providing mechanical support and electrical connections to its active and passive components. Traditionally, the PCB of a system has been considered trusted and robust during field operation. However, there are numerous recent reports on physical tampering of PCB in the field for malicious alteration of its functionality (e.g. adding/replacing a component through soldering, snooping a trace, and bypassing a connection). Through such alteration, an adversary can leak secret information from PCB or bypass security protection implemented in a system. This paper presents a novel approach to detect tampering in a PCB after it is deployed and to actively prevent system operation when tampering is detected. To our knowledge, this is the first report on active protection against PCB tampering in field. The proposed autonomous monitoring and prevention can enable active defense against physical tampering of electronic hardware, thus maintaining the integrity of a system against various security issues arising from such tampering.**

***Index Terms*—Printed Circuit Board, Physical Tampering, Active Protection.**

I. Introduction

Security of an electronic system has often been associated with the security of the software [1]. The hardware of a system that comprises of printed circuit board (PCB) and the electronic components (both active such as microchips or passive such as resistor and capacitor) has traditionally been considered trusted during field operation. However, there are a number of security issues in PCBs that are exploitable within various systems. A diverse range of possible pre and post-deployment attacks on PCB platform have been classified and discussed in [2]. An extended version of the classification is presented in Fig. 1. It specifically highlights different types of in-field attacks for PCB. The study indicates that PCBs are vulnerable to hardware Trojan attacks during design and fabrication phases. In addition to Trojan attacks, various field programmability options such as JTAG (Joint Test Access Group), probe pins, and USB (Universal Serial Bus) have allowed attackers to gain access and extract design information or leak secret keys from PCBs [2], [3]. The ease of reverse engineering the PCB allows the attackers to steal or counterfeit the design and also lets the adversary to determine various vulnerable points for attack.

In recent times, significant research efforts have been devoted in examining the security at the design and manufacturing stages of integrated circuits (ICs) and PCBs. They have also studied how to test these components throughout the manufacturing process to ensure the trustworthiness of the

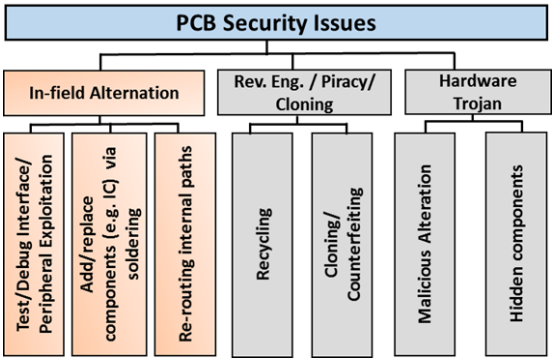


Fig. 1. Taxonomy of various security issues in a PCB during its life-cycle.

PCB and device [1], [2], [4]. Majority of these researches cover security before the product gets to the end-user. Many of these works include the prevention of cloning attacks on PCBs. A signature generation based technique has been proposed, which takes the advantage of process-induced variations in the trace impedance of PCBs and produces unique signatures for individual PCB [4]. An obfuscation based approach, which hides interconnects between the circuit components of PCBs is proposed in [6]. Other counterfeit PCB detection methods include DNA marking [7], Radio Frequency Identification (RFID) technology [8], and Physical Unclonable Function (PUF) [9], [10] based solutions.

A dominant, yet least discussed security threat to the PCB is in-field alteration. Alteration can be caused by mounting ICs, soldering wires, re-routing paths to avoid or substitute existing blocks, adding or replacing components, exploiting traces, ports or test interfaces, and in many other ingenious manners [12]. Circumventing digital rights management (DRM) by tampering the PCB of the gaming console has been the most common example of PCB tampering. Physical alteration to disable built-in restrictions allows the user to play pirated, burnt or unauthorized versions of a game on the hacked console. ModChips are devices that are used to alter the functionality or disable restrictions within a system, such as computer or video game system [12]. ModChips usually contain a micro-controller, FPGA (Field Programmable Gate Array), or CPLD (Complex Programmable Logic Device) in order to attack the host system. They are soldered into the host system and attack critical traces as can be seen in Fig. 2 (a). ModChips function through the Low Pin Count (LPC) data bus which is an industry-standard interface designed by

Intel as shown in Fig. 2 (b). The LPC bus is used for testing and debugging the Xbox during production phase [14]. Once these devices are installed they are often used for illegal purposes, such as playing illegally copied games and other forms of digital right violations. For instance, Xbox ModChips can modify or disable the built-in restrictions integrated in Xbox consoles, allowing to play pirated games in the tampered consoles. Piracy leads to loss of revenue for game developers, and a reduced budget for future games. Some high end gaming consoles like PlayStation 3 are sold at a loss with an aim to redeem the profit with the sale of games. Lack of revenue may lead to bankruptcy of the game studios and console developer companies. Furthermore, game developers would not want to risk their product on platform where piracy is prevalent. Only in UK, video game piracy through tampered consoles caused around £1.45 billion ($ 2.31 billion) loss in sales during the year 2010. This also led to around 1,000 fewer jobs in video game industry during that period [13].

ModChips are certainly not the limit to what is capable with a hardware-based attack on a system that is in the market. These hardware-based attacks pose a threat not only to a company's profits, as is the case with ModChips, but also to end-users when the product is bought and resold with such a device installed. That device can no longer be trusted as a secure device. ModChip or similar hardware-based attacks are also a threat to mobile devices. Inclusion of ModChip may allow the attacker to interfere with data between SoC and DRAM or NAND Flash. Furthermore, ModChips can capture and alter code and data which is written from SoC to memory [11]. However, the threat of in-field alteration of PCBs in terms of integrating electronic devices by exploiting PCB interfaces has barely been discussed. This paper examines a novel way in which a system can monitor in real time if tampering has occurred while the product is out in the market by measuring a certain parameter of the critical trace and comparing to the expected value. If characteristics of critical traces can be monitored to indicate this additional circuitry within the system, the attack can be prevented in real time. This type of security would benefit both the company's end-user of the product and their own profits. For this experiment the characteristic chosen to test for the purpose of monitoring was resistance.

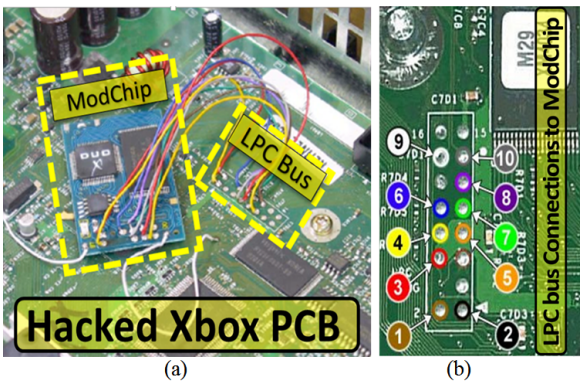


Fig. 2. Physical tampering of the PCB of a Xbox console: (a) ModChip wired with Xbox PCB through LPC bus; and (b) LPC bus with designated ModChip pin numbers.

The objective of the proposed research is to demonstrate that this additional circuitry added to a system would alter the resistances of traces in a measurable manner. This change in resistance could then be monitored in real time in order to indicate if the system has been tampered. This approach of monitoring trace resistance for tampering is shown in Fig. 3. The remainder of the paper is organized as follows. Section II will cover background on resistance measurements of printed circuit board (PCB) traces. Section III will discuss the methodology of the experiment and the results will be described in Section IV. Design implications as well as the production implementation of the design will be discussed in Section V, concluding in Section VI.

II. Background

PCB copper traces have resistive, inductive, and capacitive characteristics to them. In an attempt to keep the cost low and the PCB footprint for the additional circuitry needed for real time monitoring relatively small, we only included resistance for the purpose of the experiment. Equation 1 would dictate the initial resistance of the trace before tampering,

$$R = \rho L/A \tag{1}$$

Where R is the resistance, ρ is the resistivity of the material, i.e. copper, L is the length, and A is the cross sectional area. The addition of a single drop of solder to that trace, from which the ModChip would then be added, would cause this initial resistance to decrease. This decrease is due to the drop of solder acting as a resistance placed in parallel with the trace resistance for the length of the trace that the solder covers. The amount decreased is dictated by,

$$R = \rho_1 L_1/A_1 + \rho_1 L_2/A_1 + (A_1/\rho_1 L_3 + A_2/\rho_2 L_3)^{-1} \tag{2}$$

where ρ_1 is the resistivity of the copper trace, ρ_2 is the resistivity of the added solder, A_1 is the cross sectional area of the copper trace, A_2 is the cross sectional area of the solder drop. L_1 and L_2 are the lengths of the copper trace to either side of the solder drop and L_3 is the length of the solder drop that covers the copper trace. For simplifying the equation we assume that the cross section area of the solder drop is uniform across the copper trace. Equation 2 indicates that there is a measurable difference in resistance due to an addition to the trace and this difference will result in a net loss in resistance. Utilizing a 4-wire Kelvin method of resistance measurement, this difference can be measured in a lab. The issue with 2-wire measurements is that a portion of the probe leads are calculated into the value measured for the device under test. With the 4-wire Kelvin method, two leads are used for the current source (also called the force leads) and two leads are used for the voltmeter (also called the sense leads). Using this method the leads are placed exactly where the measurement is to be taken. The resistance of leads is then nearly completely mitigated, resulting in far more accurate and precise measurements.

III. Methodology

Determining the expected change due to additional circuity added to a trace was one of the most important aspects to this research. In order to determine what the expected change in resistance was due to additional circuitry, a PCB was fabricated by think[box] with nine straight line traces, each with the following attributes:

- Trace Width = 0.889 mm (35 mil)
- Trace Length = 177.8 mm (7 in)
- Via Diameter = 1.27 mm (50 mil)
- Via Drill Diameter = 0.70104 mm (27.6 mil)

The length was chosen as an arbitrary value that the PCB router in think[box] was capable of printing in order to begin the testing with and the width was chosen such that it would accommodate the addition of a solder drop and wire. The via drill diameter was chosen to accommodate 1/0.326 (22 AWG) wire for leads for the 4-wire measurement. Using the vias of the traces, identical length wire, 25.4 millimeters long and 1/0.326 (22 AWG), were soldered in for use as the leads to perform the 4-wire Kelvin measurements. By soldering in the test leads the contact resistance of the test probes can be reduced, as well as other environmental factors, improving the precision and accuracy. These traces are not enitirely indicative of the types of traces that would be found on a production PCB, though they serve the purpose of determining the amount of change that can be expected due to additional circuity. For this experiment, the 4-wire Kelvin measurements were completed using a HP 34401A Multimeter while at approximately room temperature, 27°C. For each measurement, a series of six measurements were taken and then averaged to achieve the final value result. Averaging six measurements for each addition to the trace decreases the affect of measurement error due to the equipment calibration or environmental factors. In order to observe the magnitude to which the resistance of a trace changed due to different additions, after the initial measurement was made, a single drop of solder was added to the middle of the trace (using solder flux to ensure the solder did not make contact with the surrounding copper) and the series of measurements were then repeated. After that, one end of a wire, 38.1 millimeters long and 1/0.326 (22 AWG), was added to the solder drop and the series of measurements were again repeated. Finally, a CD4011 NAND gate IC added to the other end of the wire, with power applied to the gate IC. The gate IC and wire were connected in various configurations to cover multiple cases, including input and output with logic low and high applied. The results, further discussed in Section IV, indicate that the configuration of the gate IC did not affect the amount of change in resistance. Fig. 4 shows an example of the types of tests performed on each of the traces.

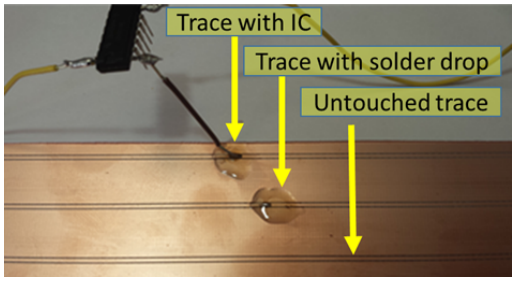


Fig. 4. An image of three of the traces under test in our experimental setup, one connected with the NAND gate IC, one with the single solder drop, and the third untouched yet.

Once the magnitude of the measurements required was determined and the degree of change to be expected was resolved, a prototype circuit was designed to measure and monitor a trace for these changes. The functional components necessary for this circuit include a microprocessor (MCU), high resolution analog-to-digital converter (ADC), a precise current source, and a method by which to indicate that the system has been tampered with. A functional block diagram depicting how these components are connected is shown in Fig. 5. The concept behind the functional block diagram is to implement a method similar to the 4-wire measurement in order to achieve the most accurate and precise measurement

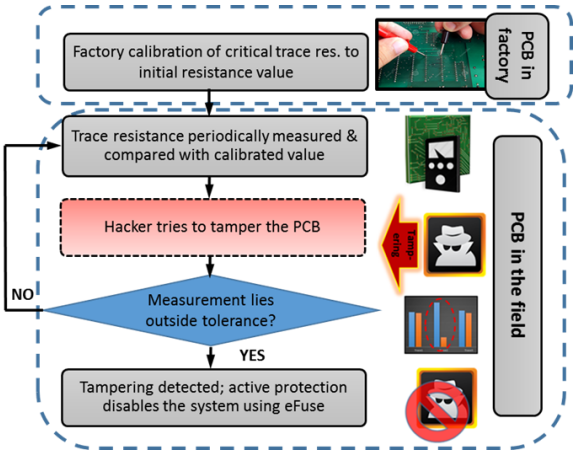


Fig. 3. Block diagram showing the general approach of hardware security through trace resistance sensing.

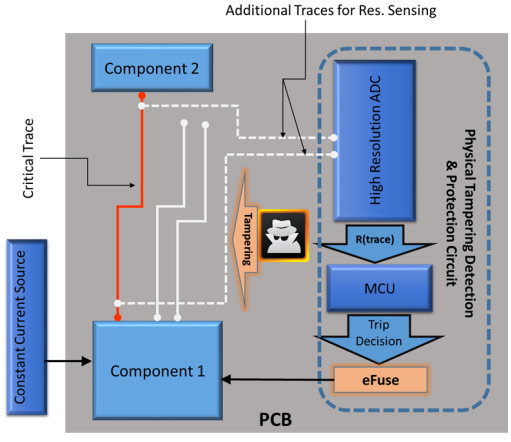


Fig. 5. A functional block diagram of the prototype tamper detection and prevention circuit on a PCB.

possible, though precision is more crucial than accuracy. One aspect of the detection circuitry that was not accounted for in this prototype circuit was that of temperature compensation. Without temperature compensation, the risk of false positives and negatives increases. This will require further research and experimentation.

For the prototype microprocessor an Arduino Uno was chosen, however it did not have a high enough resolution ADC built in for the purpose of this experiment. For the high resolution ADC, a Texas Instruments ADS1252 24-Bit ADC was used, communicating with the Arduino Uno over SPI (serial peripheral interface). The ADS1252 has a capable 23-Bits of resolution with one bit for signed readings. This magnitude of resolution combined with a 0.9 volt reference, each bit represents 107 nanovolts (i.e. 0.000000107 volts). This level of precision is required in order to achieve the degree of precision monitoring necessary while mitigating chances of false positive detection results.

IV. Results and Verification

In this section, we discuss the measurement results based on our experimental setup described in previous section. The results of the trace measurements previously mentioned in Section III validates that, over an average, there is an overall measurable negative change in the resistance values of the traces. Each additional change made to the trace would further decrease the average resistance of that trace, with two exceptions noted in the tabulated data in Table II. The average over all nine traces for the initial resistance value was 122.13 milliohms. The average change, over all nine traces, due to the addition of a single solder drop was 1.51852 milliohms. The measured absolute value of the average change from the initial value (Δ), and average percent change from the initial value $(\%\Delta)$ for each trace due to the addition of a solder drop can be found in Table I. These measurements were completed over three intervals of measuring, in groups of three (i.e. all of T1-T3 measurements were completed together, all of T4-T6 were completed together, and all of T7-T9 were completed together). The unexpected results for T6 and T7 are potentially due to the imprecise amount of solder added to each trace. These two traces had changes in resistance that were considerably larger than the other traces tested. The addition of the wire resulted in a mild net decrease in resistance from the average resistance due to the solder drop,

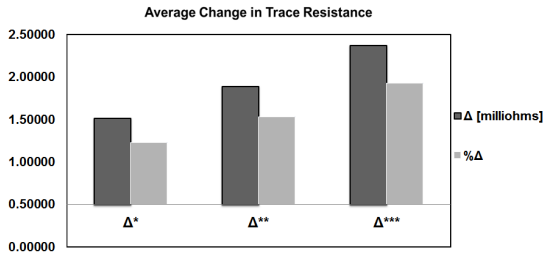


Fig. 6. Average change to resistance due to addition to a trace.

TABLE I
Average Change due to Solder Drop

Trace Designation	Average Change	
	Δ [milliohms]	$\%\Delta$
T1	0.66667	0.55633
T2	0.33333	0.2751
T3	0.66667	0.53691
T4	0.83333	0.68587
T5	0.66667	0.55402
T6	3	2.45566
T7	4.66667	3.73832
T8	1.16667	0.95109
T9	1.66667	1.32802

TABLE II
Average Change in Trace Resistance due to Addition of New Wire

Trace Designation	Average Change	
	Δ [milliohms]	$\%\Delta$
T1[1]	1.00000	0.83449
T2	0.50000	0.41265
T3	0.33333	0.26846
T4	1.16667	0.96022
T5	1.50000	1.24654
T6[2]	2.50000	2.04638
T7	6.16667	4.93992
T8	2.50000	2.03804
T9	1.33333	1.06242

thus further dropping the resistance from the initial resistance.

The measured absolute value of the average change from the initial value (Δ) and average percent change from the initial value $(\%\Delta)$ for each trace due to the addition of the wire to the solder drop can be found in Table II.

Again, the addition of the IC gate caused a further net decrease in the resistance of the traces. The measured absolute value of the average change from the initial value (Δ) and average percent change from the initial value $(\%\Delta)$ for each trace due to the addition of the gate IC to the wire can be found in Table III. The gate IC was connected as an input for traces T1-T2 and T5-T6. Traces T3-T4 were configured as output logic low and traces T7-T9 were configured as output logic high. It is clear from the results that the configuration of the gate IC did not matter for the average change in resistance of the trace. The results show that there will be a net decrease in the resistance of a trace due to additional circuitry and that with precise and accurate measurements, these reductions in resistance can be measured. Each of the above tabulated results were then averaged over all nine traces for each respective table to achieve the net average change and average percent

[1] *This value was actually an unexpected net increase in resistance from the initial resistance.*

[2] *This value was actually an unexpected net increase in resistance from the previous resistance.*

TABLE III
AVERAGE CHANGE IN TRACE RESISTANCE DUE TO ADDITION OF AN IC THROUGH SOLDERING

Trace Designation	Average Change	
	Δ [milliohms]	%Δ
T1	2.00000	1.66898
T2	0.50000	0.41265
T3	0.83333	0.67114
T4	2.16667	1.78326
T5	1.83333	1.52355
T6	5.16667	4.22920
T7	5.33333	4.27236
T8	1.83333	1.49457
T9	1.66667	1.32802

change that is expected from addition of single solder drop to a trace, then a wire to that solder drop, and a gate IC added to the wire. These average changes are illustrated in Fig. 6, where Δ^* represents the change from the initial value due to the solder drop, Δ^{**} represents the change from the initial value due to the added wire, and Δ^{***} represents the change from the initial value due to the addition of the gate IC. The average change for the addition of a single solder drop to a trace over all nine traces was 1.51852 milliohms, with an average percent change of 1.23126%. For the addition of the wire, the average change in resistance from the initial value was 1.88889 milliohms, with a average percent change of 1.53435%. When the gate IC was added, the average change in resistance was 2.37037 milliohms, and an average percent change of 1.93153%. The minimum change in the average resistance over the series of six measurements was 0.33 milliohms (i.e. 330 micro-ohms), with a percent change of 0.26846%. The prototype circuit was then built and tested around the expected results based on the previous experiment. For the purpose of the current source, a 0.9 volt regulator (with a measured value of 0.897 volts) (part number NCP565) combined with a precision 1 ohm resistor (measured value of 1.0053 ohms averaged over six measurements) were used and the calculations for the measured resistance were done utilizing Ohm's Law. The sense resistor is connected to the voltage regulator and the trace resistance. The other end of the trace is connected to ground. Using the measured voltage at the sense and trace resistor connection, $V_{measured}$, the current, I, through the resistors can be calculated using Equation 4, Where V_{reg} is the regulated voltage value and R_{sense} is the value of the sense resistor, 1.0053 ohms. Using this calculated current, I, and the measured voltage again, $V_{measured}$, the value of the trace resistance, R_{trace}, can be calculated using Equation 3,

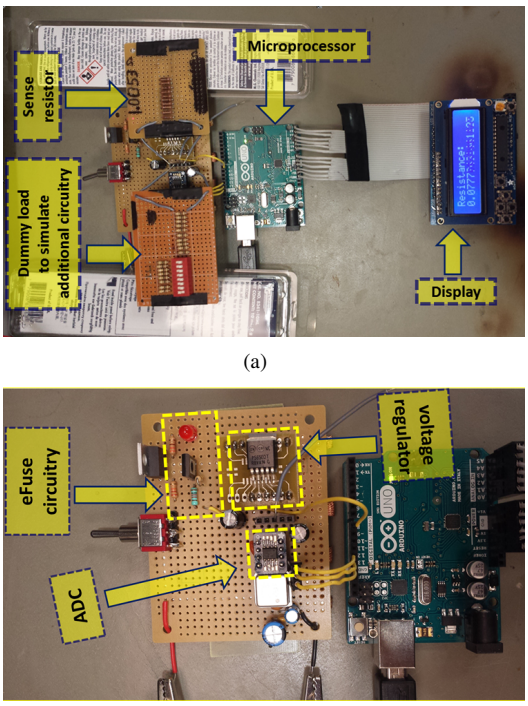
$$R_{trace} = V_{measured}/I \tag{3}$$

Utilizing Equation 3 and 4, the value of the trace resistance is calculated in order to then monitor for additional circuitry.

For the prototype circuit, the"trace" resistance was created using ten 1 ohm resistors in parallel to begin with a relatively small resistance, further more eight 1 ohm resistors could be individually turned on and off in parallel to further alter the resistance. By turning on seven of the switches, adding in seven more 1 ohm resistors in parallel with the initial ten, the average resistance, over six measurements, of the"trace" under test was 67.2 milliohms.

$$I = (V_{reg} - V_{measured})/R_{sense} \tag{4}$$

By turning on the eighth switch, the average resistance dropped by 2.2 milliohms down to 65.0 milliohms, approximately a 3.3% difference. Due to the minimum percent change in resistance that was measured in the experiment, a change of 0.26846%, the tolerance of allowed drift in resistance for the prototype circuit was set to 0.25%. This allowed for minor differences between readings to not trip the microprocessor into the detected/tripped state, but if a change in resistance was detected above 0.25% the circuit would enter the detected/tripped state. When the circuit starts up, it automatically calibrates the expected resistance value to the initial reading of the ADC, after which it enters a monitoring state. For each resistance value calculated, one hundred ADC readings are taken, then the upper and lower 10% outliers are discarded, and the remaining eighty values are averaged to get the"true" ADC reading value. This is how the calibration of the initial value is done which is used during the monitoring state. By removing the outlier values and averaging multiple readings, errors in readings and fluctuations due to environmental factors are reduced. Once in the monitoring state, the percent change from the calibrated value to the read value is then computed



(a)

(b)

Fig. 7. (a) The prototype circuit used in our experimental measurements; (b) the same circuit without the sense and trace resistors attached.

to determine if the circuit should enter the detected/tripped state. The prototype circuit built functions within the required precision to properly operate under these tolerances, tripping when the last measured value from the ADC reads outside of the 0.25% tolerance. The prototype circuit can be seen in Fig. 7(a) and 7(b).

V. Discussion

The current prototype circuit design has two potential lapses in the design where it does not account for temperature and aging of the product. One method to compensate for the change in the resistance due to temperature would be to use a temperature sensor in the design. A temperature sensor can be integrated into the design for low cost and would be able to utilize the existing microprocessor for simple calculations to adjust the reading for the current temperature, as is discussed in [5]. Another method to compensate for changes due to temperature, and potentially aging, would be to utilize a common mode signal. An equivalent trace would be compared to in the case of a common mode signal, such that the effects of temperature, and potentially aging, would create a common mode signal. The changes in aging would also potentially be over come simply by the fact that the changes due to aging will be less significant in comparison to simple fluctuations in readings due to component tolerances. If aging is of greater concern, conformal coating or potting can be used to further mitigate the effects of aging on the resistance of the trace.

By implementing the basic functional block diagram components of Fig. 5, utilizing high precision components, the real time monitoring for additional circuitry to a system can be achieved. This design can be implemented into a PCB with a relatively small footprint added to the overall PCB design and simple factory calibration of the initial trace resistance. This initial trace resistance value will then be stored in protected, nonvolatile memory of the microprocessor. By utilizing an electronic fuse (eFuse), the system could be rendered inoperable when tampering is detected, if that is the desired outcome to a positive. Rendering the system nonfunctional would prevent sensitive information from being stolen or illegal activities from taking place. Furthermore the eFuse could be placed on an internal layer of the PCB, preventing the attacker from simply replacing or bypassing the eFuse.

For a more robust and comprehensive coverage of traces, mitigating false positives, multiple traces within a given system could be monitored. This could be done using a multi-channel ADC or multiple ADCs, if necessary. With a multi-channel ADC, each trace could be checked independently, cycling through all channels of the ADC, thus monitoring multiple traces in series. With multiple ADCs, the crucial traces could potentially all be monitored in parallel. When a set number of traces are outside of the allowed tolerance for each trace, the circuit could trip and render the system nonfunctional. However, this defense mechanism needs to be protected from additional tampering that would render it useless. This could be done through a number of methods. The crucial components to this defense mechanism could be intentionally placed within internal layers of the PCB, physically shielding the components of the defense mechanism from tampering. Another method could include implementing the defense mechanism within the application specific IC (ASIC) of the product. By implementing the sensing and decision making mechanism within the ASIC, the crucial components are again physically protected from tampering.

VI. Conclusion

We have presented a novel approach for active protection against physical in-field tampering of PCBs. Through experimental measurements on custom PCB circuits, we have shown that a low-overhead trace-resistance based approach can detect different types of physical tampering in PCB. With the proliferation of embedded systems in diverse applications, physical tampering is becoming a dominant attack mode to alter hardware functionality, e.g. bypassing the DRM protection of a gaming console. The proposed real-time monitoring circuit can effectively protect against such attacks in a manner that defeats an attacker's objective. The experimental results show that a malicious alteration is measurable from a single drop of solder to addition of a new microchip. By judiciously routing the additional traces through the internal layers of a PCB, the proposed solution can be protected from potential compromise. Moreover, to minimize the overhead and enhance the security, one can use existing processor or FPGA in a PCB to implement the tamper detection/prevention module.

References

[1] S. Bhunia, M. Hsiao, M. Banga, S. Narasimhan, "Hardware Trojan Attacks: Threat Analysis and Countermeasures", *Proceedings of the IEEE*, 2014.

[2] S. Ghosh, A. Basak, and S. Bhunia, "How Secure are Printed Circuit Boards against Trojan Attacks?", *IEEE Design & Test*, 2014.

[3] F. Domke, "Blackbox JTAG Reverse Engineering, 2009", [Online]. Available: http://events.ccc.de/congress/2009/Fahrplan/events/3670.en.html.

[4] F. Zhang, A.Henessy, and S. Bhunia, "Robust Counterfeit PCB Detection Exploiting Intrinsic Trace Impedance Variations", 33rd *IEEE VLSI Test Symposium*, 2015.

[5] S. Ziegler, R. C. Woodward, H. H. C. Iu, L. J. Borle, "Investigation into Static and Dynamic Performance of the Copper Trace Current Sense Method", *IEEE Sensors Journal*, 2009.

[6] Z. Guo, J. Di, M. Tehranipoor, D. Forte, "Investigation of Obfuscation-based Anti-Reverse Engineering for Printed Circuit Boards", *Design Automation Conference*, 2015.

[7] M. Miller, J. Meraglia, and J. Hayward, "DNA Marking and Authentication: A Unique, Secure Anti-counterfeiting Program for the Electronics Industry", *Applied DNA Sciences*, Stony Brook, NY, USA.

[8] S. Devadas et al. "Design and Implementation of PUF-based "Unclonable" RFID ICs for Anti-counterfeiting and Security Applications", *IEEE International Conference on RFID*, 2008.

[9] G.E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation", *DAC*, 2007.

[10] A.R. Krishna et al. "MECCA: A Robust Low-Overhead PUF using Embedded Memory Array", *CHES*, 2011.

[11] "Security Threats on Embedded Consumer Devices", version 1.1, Open Mobile Terminal Platform, 28th May, 2009.

[12] Modchip: Wikipedia, the free encyclopedia. [Online]. Available: https://en.wikipedia.org/wiki/Modchip.

[13] D. Whitworth (21 Jan 2011) BBC, [Online] Available: http://www.bbc.co.uk/newsbeat/article/12248010/gaming-industry-lose-billions-to-chipped-consoles.

[14] J. Grand et al. "Game Console Hacking: Have Fun While Voiding Your Warranty", Syngress, 2005.