AFRL-RI-RS-TR-2021-145

PDN-PULSE: UBIQUITOUS AND INHERENT ANOMALY DETECTION WITH CROSS-LAYER INTERACTIONS OF POWER DELIVERY NETWORK

WASHINGTON UNIVERSITY

AUGUST 2021

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This report is available to the general public, including foreign nations. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2021-145 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE CHIEF ENGINEER:

/ S /
SERGEY PANASYUK
Work Unit Manager

/ S /
JAMES S. PERRETTA
Deputy Chief, Information
Exploitation & Operations Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
AUGUST 2021	FINAL TECHNICAL REPORT	JUL 2020 – APR 2021

4. TITLE AND SUBTITLE

PDN-Pulse: Ubiquitous and Inherent Anomaly Detection with Cross-Layer Interactions of Power Delivery Network

5a. CONTRACT NUMBER
FA8750-20-1-0505

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
AF/Other

6. AUTHOR(S)

Xuan 'Silvia' Zhang
Yier Jin

5d. PROJECT NUMBER
DEST

5e. TASK NUMBER
RO

5f. WORK UNIT NUMBER
02

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

PRIME
Washington University in St. Louis
1 Brookings Dr.
St. Louis, MO 63130

SUB
University of Florida
968 Center Dr.
Gainesville, FL 32603

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory/RIGB
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSOR/MONITOR'S REPORT NUMBER
AFRL-RI-RS-TR-2021-145

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The sophistication of today's computing system gives rise to the increasing threats of malicious and coordinated attacks targeting both software and hardware vulnerabilities. We successfully conduct fundamental research on building a holistic anomaly detection framework by leveraging the inherent cross-layer system infrastructure of power delivery network (PDN). PDN is an essential and ubiquitous component in electronic systems. Our meth-od fundamentally relies on detecting the changes of PDN impedance profile induced by anomalies at different levels. To demonstrate its effectiveness, we conducted proof-of-concept experiments on customized System-on-Chip (SoC) development boards and COTS products, both with successful detection results. We have further developed a system-level security-oriented PDN modeling tool (PowerScout) and a systematic benchmarking method (PCBench) to comprehensively and quantitatively evaluate printed circuit board(PCB)-level attacks. Overall, our project has thoroughly explored the potential of a holistic PDN-based approach for system anomaly detection.

15. SUBJECT TERMS

Trojan, PCB, Supply Chain, modeling, simulation, sensor fusion, and machine learning

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			**SERGEY PANASYUK**
U	U	U	UU	23	19b. TELEPHONE NUMBER (*Include area code*) **N/A**

TABLE OF CONTENTS

LIST OF FIGURES

1.0 SUMMARY

The sophistication of today's computing system gives rise to the increasing threats of malicious and coordinated attacks targeting both software and hardware vulnerabilities. To address this security challenge in this project, we successfully conduct fundamental research on building a holistic anomaly detection framework by leveraging the inherent cross-layer system infrastructure of power delivery network (PDN). PDN is an essential and ubiquitous component in electronic systems. It connects every component across multiple levels (e.g. chip, package, board), and hence is able to comprehensively sense any disturbances within the integrated system. In this project, we developed PDN-Pulse, a unified detection framework for malicious hardware insertions across chip-, board-, and system-levels in commercial-off-the-shelf (COTS) products. Our method fundamentally relies on detecting the changes of PDN impedance profile induced by anomalies at different levels. To demonstrate its effectiveness, we conducted proof-of-concept experiments on customized System-on-Chip (SoC) development boards and COTS products, both with successful detection results. We have further developed a system-level security-oriented PDN modeling tool (PowerScout) and a systematic benchmarking method (PCBench) to comprehensively and quantitatively evaluate printed circuit board(PCB)-level attacks. Overall, our project has thoroughly explored the potential of a holistic PDN-based approach for system anomaly detection.

2.0 INTRODUCTION

The sophistication of today's computing system gives rise to the increasing threats of malicious and coordinated attacks targeting both software and hardware vulnerabilities [1]–[3]. To address this security challenge, we propose to conduct fundamental research on building a holistic anomaly detection framework by leveraging the inherent cross-layer system infrastructure of power delivery network (PDN) that is an essential and ubiquitous component in any electronic systems. Such framework would not only provide a unified approach to detect anomalous software behaviors and malicious hardware insertions across chip-, board-, and system-levels in commercial-off-the-shelf (COTS) products, it also has the advantage of being light-weight and compatible with legacy systems by reusing the feedback/sensing mechanism and power management knobs inherent in the PDN subsystems. Existing detection methods often focus on a single system layer and cannot easily extend to spot anomalies across different design layers [4]–[7]. For example, chip-level hardware Trojan detection adopts different methods from those at the board level; whereas software-based anomaly detection methods often have high overheads which cannot be applied to resource constraint devices. Therefore, a series of different detection approaches are needed in order to ensure the trustworthiness of a complex platform which may contain multiple chip modules along with a number of discrete components on a multi-layer printed-circuit board (PCB) board.

To overcome the limitations of existing one-hot detection schemes, we propose a unified anomaly detection approach leveraging an inherent full system-level infrastructure which exists universally in any complex System-on-Chip (SoC) and COTS products, the Power Delivery Network (PDN). The proposed unified PDN framework, named PDN-Pulse, will characterize the PDN impedance profile. Specifically, we will try to detect hardware anomalies including hardware Trojans, and counterfeit PCBs.

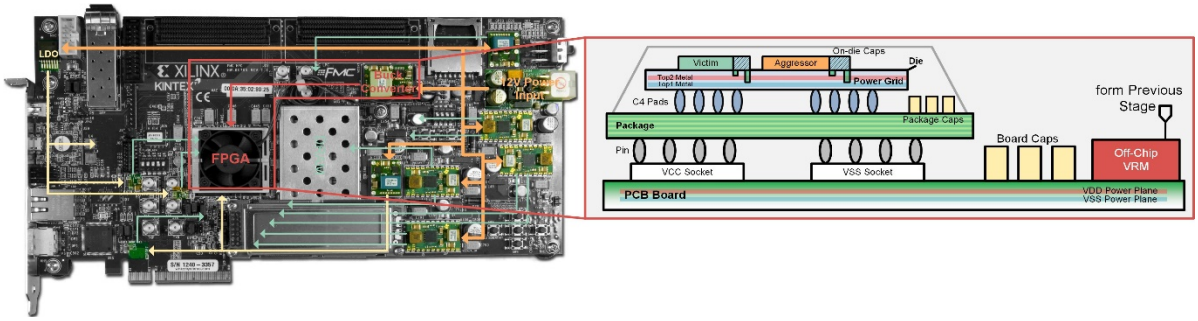

Figure 1. PDN architecture of a sample FPGA implementation.

The proposed unified framework will provide a comprehensive assurance of COTS security across all design layers in the entire system. It is the first detection method that can be generalized for monitoring full-system cross-layer anomalies. Our proposed PDN-Pulse aims to construct a unified detection framework built upon existing PDN infrastructure using both frequency and time-domain side-channel analysis. The PDN is an essential subsystem in modern electronic systems that is designed to distribute stable supply voltage and reliable electric power to each functional unit in a complex integrated system. Figure 1 provides an example of the organization and structure of the PDN across multiple physical levels from the board to the chip in a real field programmable gate array (FPGA) implementation. It contains board-level voltage regulator modules (VRMs), interconnects from the VRMs to the package pins and bonding pads, on-chip power grids to distribute power locally across the die, and decoupling capacitors along various stages of the PDNs. The PDN connects every part across multiple levels (e.g. chip, package, board) of the system, and

hence is able to comprehensively sense any disturbances in the integrated ecosystem, much like the role arteries/veins play in human body to circulate blood and transport oxygen and nutrients. Therefore, even minuscule changes to the system, be it hardware insertion at the board, package, or chip levels, or power management abnormalities initiated in the software domain, can affect the PDN characteristics and load current behaviors simultaneously and manifest themselves in accurate PDN measurements. This sensitivity of the PDN has in fact already been exploited in part by attackers for invoking side-channel information leakages.

Different from existing PDN exploitations, we plan to leverage such PDN sensitivity for hardware anomaly detection. PDN-Pulse's ability to detect anomalous behavior relies fundamentally on the PDN characteristics. Figure 2 illustrates the typical frequency response profile of an example PDN, where the X-axis is the frequency and the Y-axis represents the magnitude of equivalent complex impedance of the PDN. Such PDN profile can serve as a natural candidate for system fingerprint that can uniquely identify the status of the system in normal operation. Anomalies at different levels will inevitably introduce changes to the original PDN profile, thus can be modeled either as exogenous resistor-inductor-capacitor (RLC) components or abnormal load currents, as conceptually illustrated in Figure 2. The proposed PDN-Pulse utilizes measurements to monitor a variety of subtle changes in the PDN profile to speedily identify system anomaly at any stage and across any level in an SoC/COTS platform.

Compared to existing anomaly/intrusion detection methods, our PDN-Pulse framework has several unique advantages:

- First, we can provide a unified approach for detection across the system stack, from user space in the software domain all the way to different system levels in the hardware domain;
- Second, PDN-Pulse has the potential for higher detection accuracy by using both frequency and time domain information;
- Third, PDN-Pulse implementation has low overhead without modification to existing SoC/COTS platform.

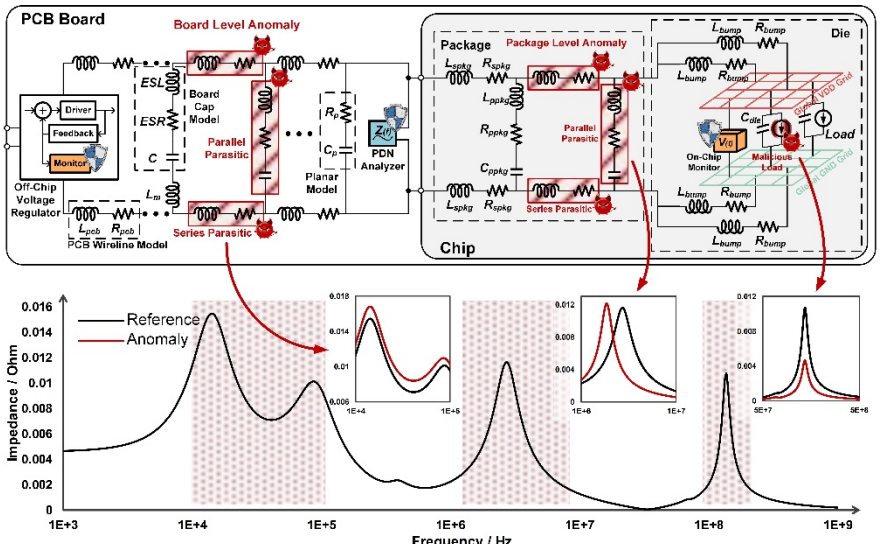

Figure 2. A sample PDN circuit model and its profile in the frequency domain.

3.0 METHODS, ASSUMPTIONS, AND PROCEDURES

3.1 PDN-Pulse Proof-of-Concept Experiment

To validate the capability of PDN-Pulse, we first obtain the proof-of-concept results and validated the both off-line detection methodology and the power supply background noise based on-line detection method on custom demo PCB boards. Two types of board-level anomaly have been implemented on the PCB and are detected by comparing the PDN impedance profiles and noise spectrum.

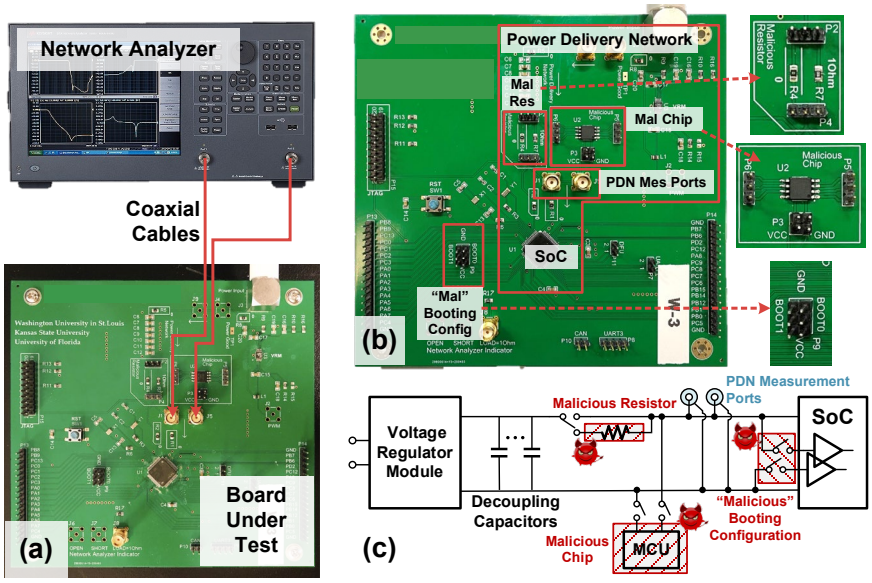

Figure 3 (a) The setup for measuring the PDN impedance of customized board. (b) The layout of the customized board with Trojans inserted. (c) The simplified PDN schematic of the board.

Figure 3 (b) shows the layout of the customized board with Trojans inserted. The customized board designed for demonstration is a microcontroller development board which contains a STM32 ARM-based SoC chip and its peripheral circuit. As the proof-of-concept board, two subminiature version A (SMA) adapters connected to the PDN are added to the PCB. The board can be directly connected to the vector network analyzer (VNA) using coaxial boards. An 1Ohm malicious sampling resistor and a malicious microcontroller (MCU) ATtiny85 chip are implemented in the system with switches to set up different configurations. The ATiny85 has the current consumption as small as 300uA, which has been used in the attack to the firewall board [1]. Thus three different configurations can be set for the demo board. When configured in Golden Model, none of the malicious components are included into the original circuit, which works as the reference design. While in Malicious Resistor, the 1Ohm malicious sampling resistor is in-series connected to the PDN to enable the power side-channel attacks such as correlation power analysis (CPA) and differential power analysis (DPA) [8], [9]. For the Malicious Chip configurations, the ATtiny85 is powered on with the its power supply pins connected to the PDN and the its functional pins connected to the target signal wireline. The ATtiny85 can perform multiple attacks. For example, it can monitor the communication of the system bus, and once triggered, drive the ERASE pin to delete the firmware of the SoC. The PDN of the system is designed according to the guidance of the SoC datasheet. A board switching VRM converts the 5V system supply to 1.2V to power the SoC. A decoupling capacitor array is implemented between the VRM and the SoC. Besides the

malicious resistor for power side-channel attacks, the ATtingy85 also need to be connected to the PDN due to it is not self-powered.

For the experimental setup of off-line detection using VNA (as shown in Figure 3 (a)), we use the Keysight E5063A VNA, which supports the measurement from 100KHz to 3GHz. The bandwidth of interest is 100KHz to 1GHz. The VNA is set to 2-port shunt-through measurement. Two SMA cables are used to connect the Port1 and Port2 to the J1 and J5 of the demo board respectively. Before the measurements, the standard 2 port calibration is performed on VNA to calibrate the errors caused by the SMA cables. In this experiment, we measure the PDN impedance of several custom demo boards from 100KHz to 1.5GHz under different configurations. For each measurement, the conversion from S-parameters and Z-parameter is performed.

For the experiment of on-line detection based on measuring the spectrum of power supply noise, the Keysigth N9020B spectrum analyzer is utilized with enabling built-in low noise pre-amplifier, which can support the measurements form 10Hz to 3.6GHz. The bandwidth of interest for this experiment is from 100MHz to 1.1GHz. Meanwhile, the power supply Tektronix 2231A-30-3 connected to the board through a power cable. An SMA cable connects the spectrum analyzer and the J1 port of the demo board. The board is set to idle mode without any programs running. Similarly, the background power noise spectrum of the PDN is measured among the demo boards under different configurations. Both the Trace Average and the Power Average are enabled. We also implement the average filter to the measured data to smooth the curve. Three boards are measured and for each board we measure 2 times.

Moreover, we test PDN-Pulse on the COTS PCBs - Arduino Uno. It is an open-source design of a general microcontroller development board based on the ATmega328P. This board is popular in the market for its low cost. It has been fabricated and sold by many manufacturers. We purchase a total of 36 Uno boards from three different vendors (13 from each vendor): Arduino.cc, Elegoo, and Kuman. All three designs share the same schematic and almost the same layout. In our experiment, we mimic the board-level counterfeiting situation by referring Elegoo and Kuman Arduino Uno boards as suspicious boards while official Arduino Uno boards from Arduino.cc are treated as genuine ones. We measure the PDN of the 5V voltage domain which is the main supply voltage of the PCB and perform anomaly detection.

3.2 Systematic Benchmarking Method

When conducting the experiments of testing PDN-Pulse on COTS PCBs, we notice that even though board-level attacks are emerging hardware threats [10], [11], the attack and defense techniques at the board level have not yet been systemically explored and thus require a thorough and comprehensive investigation. In the absence of standard board-level attack benchmark, current research on perspective countermeasures is likely to be evaluated on proprietary variants of ad-hoc attacks, preventing credible and verifiable comparison among different techniques.

To comprehensively and quantitatively evaluate PDN-Pulse, in this task, we systematically define and categorize a broad range of board-level attacks. For the first time, the attack vectors and construction rules for board-level attacks are developed. Four rules are proposed to facilitate the development of board-level benchmarking.

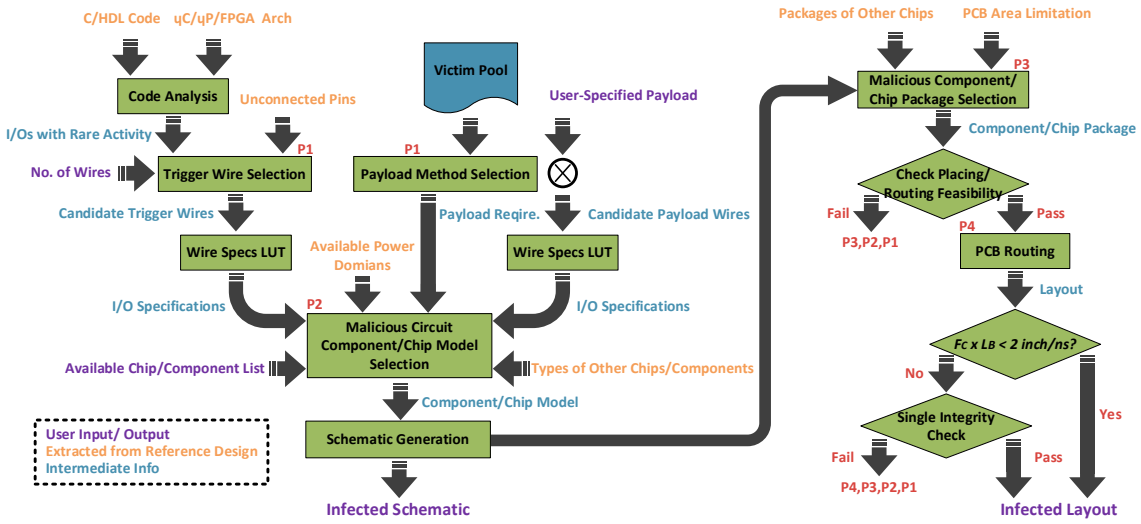

Figure 4 : Benchmark Generation Workflow for Board-Level Attacks (P1 - P4 are the steps of the workflow)

Based on these rules, we develop a methodology for generating benchmarks of board-level attacks and a workflow using the method (see Figure 4). The first step is to collect the signals with rare activities for trigger selection. The candidate trigger wires come from two parts: inputs/outputs (I/Os) with rare activities and unconnected pins of the chips. Since the I/O activities of the chips are highly related to the pro-grams of the chips, we perform code analysis based on the code and the architecture of the chips. Wires are further selected as candidate trigger wires (note that the number of trigger wires are decided by attackers). Then the specifications of the wires are looked up from the reference design. Meanwhile, the payload can be specified by attackers or picked from the victim pool. In this step, both the traditional digital Trojans and the attacks based on analog properties are considered for the payload. Once the candidate payload wires are selected, corresponding specifications are also looked up from design files and datasheets. The malicious circuit is designed based on the information of trigger/payload wires specifications, available power delivery system voltage domains, types of other chips/components, and the available chips/components. If there exists a malicious circuit design that meets all these rules, an infected schematic can be generated. For layout level benchmark, packages of the malicious circuit are selected according to the packages of other chips (PCB spare area is a constraint here). Then the placing and routing feasibility are checked, following the signal integrity check. The signal integrity check is not necessary for the board with low speed. Therefore, we set up a threshold to determine whether to perform the check, as:

$$k \times L_b \div 6\ \text{inch/ns} < 1/f_c \quad (1)$$

where f_c is the clock frequency of the signal, L_b is the board perimeter, and k is the safety factor. If the infected layout passes the checks, the benchmark can then be generated. Otherwise, we will return to previous steps (marked as P1, P2, P3, and P4) and re-design the malicious circuit.

3.3 System-Level Security-Oriented PDN Modeling Methodology and Simulation Tool

The PDN-Pulse is based on detecting the changes of characteristics (e.g., impedance profile, background noise spectrum) of PDN. To increase the performance of PDN-Pulse, we further develop a security-oriented PDN modeling methodology and simulation tool named PowerScout. Pow-

erScout performs fast nodal analysis of complex PDNs at the system level to quantitatively evaluate the severity of side-channel vulnerabilities. We validate PowerScout by replicating PDN side-channel attacks in literature through simulation results. Further, we are able to quantitatively measure the security impact of PDN parameters and configurations. For example, towards information leakage, removing near-chip capacitors can increase intra-chip information leakage by a maximum of 23.23dB at mid-frequency and inter-chip leakage by an average of 31.68dB at mid- and high-frequencies. Aided by PowerScout, we are able to find new features of the PDN to help perform anomaly detection. We prove that the new feature can detect the malicious changes that are not able to detect from circuit perspective.

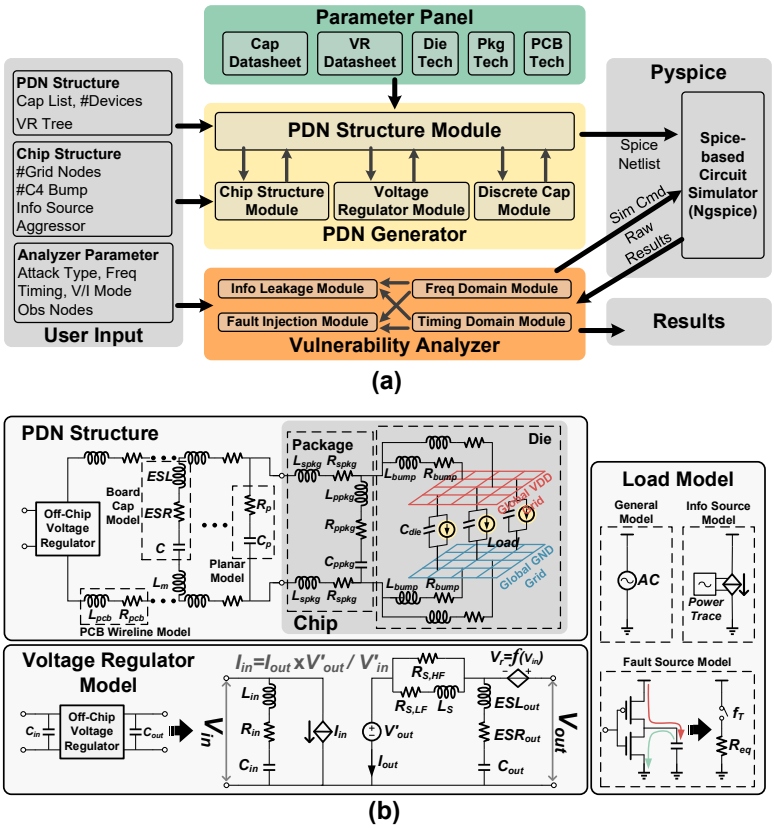

Figure 5 (a) The system diagram of the proposed PowerScout framework. (b) Security-oriented modeling of different PDN components.

The diagram of the proposed PowerScout is shown in Figure 5 (a). PowerScout contains three main parts: the parameter panel, the PDN generator, and the vulnerability analyzer. Users can call modules inside PowerScout with pre-defined PDN templates, which determines the topology of the PDN. The parameter panel abstracts the PDN parameters from electronic component datasheets and technology libraries. For example, for the chip-level PDN topology, users can define several parameters such as the number of the power grids and controlled collapse chip connection (C4) pads and the loads' types and locations. Given these inputs, the developed PDN generator will automatically generate and simulate a full-system PDN netlist that specifies the complex hierarchical network. The raw outputs are parsed according to user-defined security analysis objectives and the side-channel vulnerability results are then reported by the vulnerability analyzer.

The structure of PDN model is shown in Figure 5 (b). The model aims to fully reflect the power supply paths for critical devices with sufficient details. The board-level supply wireline is modeled as an inductor and a resistor, whose parameters depend on its length, width, and metal material characteristics. The PCB planes use the planar model with lumped capacitor and resistor, since the distributed effect is minimal at this scale. For the board-level capacitors, we model the characteristics of each capacitor. The frequency response of a single real capacitor is a band-pass filter instead of an ideal low-pass filter due to the parasitic effects. The capacitor is thus modeled as the equivalent series inductor (ESL), equivalent series resistor (ESR), and an ideal capacitor. For the chip-level PDN, we use the widely accepted package and die models [12], [13]. The package is modeled as an RLC network, and the C4 bumps are modeled as parallel RL pairs that connect the grid to the package. The on-chip grid (i.e., the die model) is represented as an RL network. The on-chip capacitance is evenly distributed between the power supply (VDD) and ground (GND) grids. In previous works and industrial models [14], [15], VRMs are typically modeled as a fixed voltage source or a fixed voltage regulator in series connected to the equivalent inductor, capacitor, and resistor. But this kind of model is not suitable for security-oriented PDN modeling since it ignores the interactions between different voltage domains. In PowerScout, we model the bi-directional interactions of different VRM topologies, including low-dropout regulators (LDOs), buck converters, and switched-capacitor converters. We also provide three different load models that are suitable for different attack types and analysis objectives.

4.0 RESULTS AND DISCUSSION

4.1 Results of Proof-of-Concept Experiment

Figure 6 shows the proof-of-concept results of anomaly detection based on VNA. We first measure the PDN impedance of 6 boards under Golden Model configuration to decide the bound for process variations. The $\bar{x} \pm 3\sigma$ are set as the upper and lower bounds, where the $\bar{x}$ is the average value and σ is the standard variations of the data. The bound is used to setup the region of abnormal impedance profile. It can be seen that there is a large process variation at low frequency (<1MHz) and the high frequency (> 200MHz) due to the noise and electromagnetic (EM) infections. The process variation at the mid frequency (1MHz< f< 200MHz) range is small and can provide accurate detection. Under Malicious Resistor configuration, with 1Ohm malicious resistor included, the impedance lower than 10MHz increase significantly. While under Malicious Chip configuration. The impedance profile at mid-frequency range also significantly changed. For both types of anomaly, we can directly identify the malicious modifications by measuring the PDN impedance profile, which validate the off-line detection methodology.

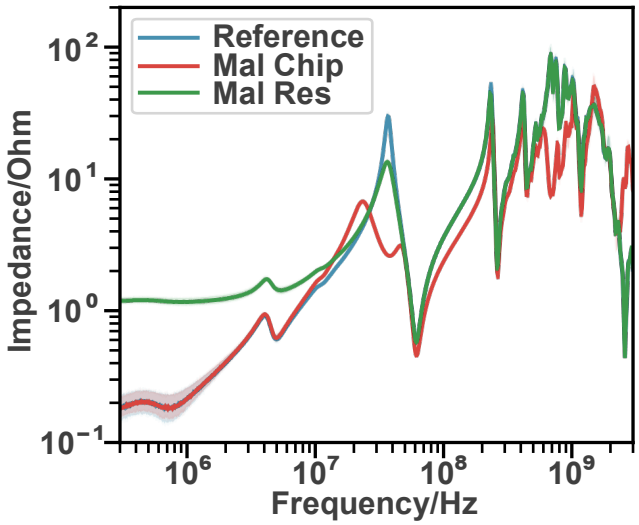

Figure 6 Proof-of-concept results of customized PCB showing PDN sensitivity for board-level hardware Trojans

Figure 7 shows the results on-line detection by using spectrum analyze to measure the power noise spectrum. According to the background noise spectrum under Golden Model configuration, the bound of process variations is also calculated as $\bar{x} \pm 3\sigma$. As configured in Malicious Chip the noise spectrum is changed, where the changes are introduced at the range from 600MHz to 1.1GHz. This malicious modification can also be directly identified through the visual examination of the noise spectrum. Note that we find the SA-based method cannot detect the sampling resistor due to its quite small noise contribution.

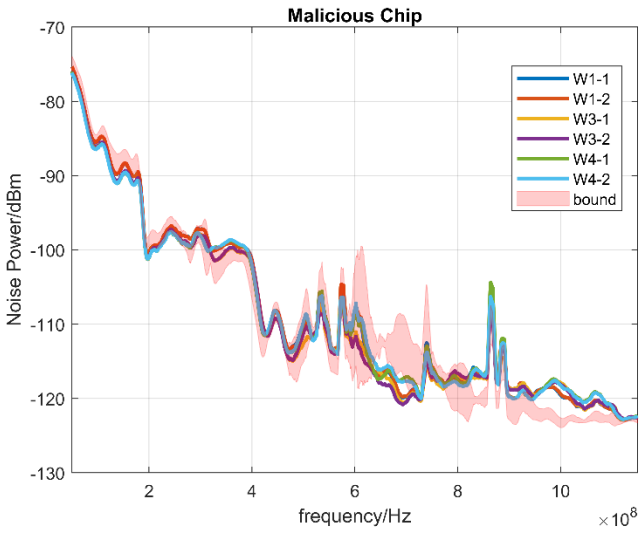

Figure 7 Proof-of-concept results of customized board using spectrum analyzer. The colored lines are the spectrum when malicious chip is inserted into the board.

Figure 8 illustrates the results of testing PDN-Pulse on the COTS PCBs - Arduino Uno. We show the impedance profile comparison of boards from three vendors, respectively. During the measurements, we notice that there are two batches of Elegoo boards. The two batches of Elegoo boards are marked as Elegoo-I and Elegoo-II. They could either be different versions of the boards, or just due to the changes of passive components vendors. The green, red, blue, and orange lines represent the mean impedance profile of the boards from Arduino, Elegoo-I, Elegoo-II, and Kuman, respectively. We cannot recognize any differences by examining the appearance of boards and discrete components. However, we can confirm the two batches from the impedance profiles. Since the differences of impedance profiles are mostly at the low frequency below the board resonance region, we infer that for the two types of boards they have the same PCB layout, but the discrete components may be from different vendors or have different specifications. In addition, we can distinguish the Arduino boards and Kuman boards from the impedance profiles. Therefore, based on the PDN-Pulse framework, we can identify not only the same PCB design manufactured by different vendors, but the PCBs of different batches even from the same manufacturer. We further perform the counterfeit detection by examining whether the PDN impedance profile of board-under-test exceeds the $\bar{x} \pm 3\sigma$ bound of genuine Arduino boards. We test 36 boards and achieve up to 93.75% PD (possibility of detection) and 0% PFA (possibility of false alarm) with 5 training samples and 31 testing samples.

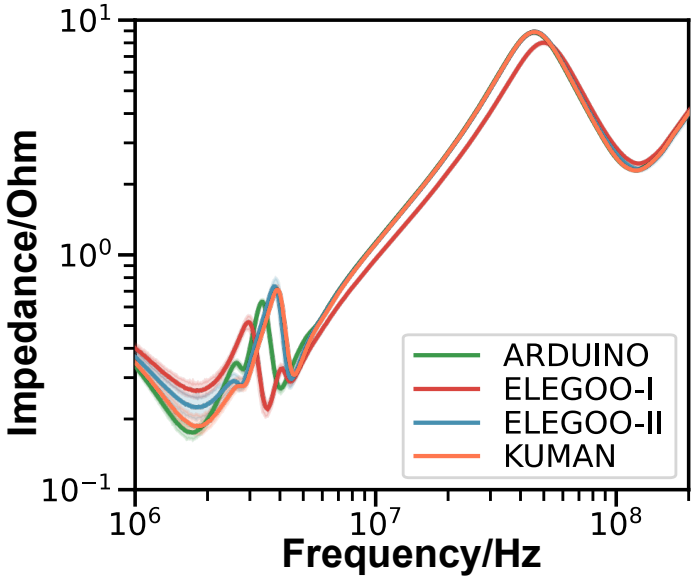

Figure 8 The comparison of impedance profile of Arduino Uno boards from different vendors.

4.2 Implementation of Systemic Benchmarking Method

To facilitate the development of board-level attack benchmarks, representative circuit boards are chosen as the victim designs. Open-source hardware projects are mainly selected due to their modern design styles, the availability of PCB designs as well as detailed documents, firmware, and/or application software. As a result, researchers can easily reconstruct the board-level security evaluation benchmarks. Based on the workflow, we can generate a variety of different board-level attacks to compile a full set of benchmark suite. In this project, we implement two sample benchmarks: the benchmark based on Arduino Due micro-processor development board, and the benchmark based on the A13-OLinuXino single board computer (see Figure 9). For each benchmark, we insert three different types of Trojans. More benchmarks can be found at https://github.com/xz-group/PCBench.

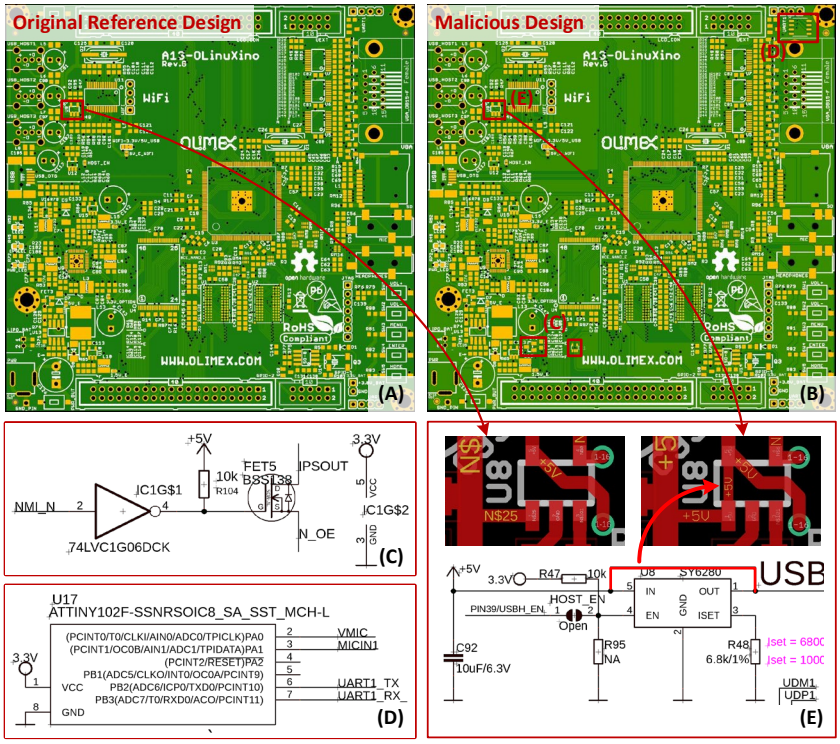

Figure 9 The PCB layout of (a) original reference design and (b) malicious design of Olimex A13-OLinuXino; (c) The malicious circuit receives the interrupt signal from a real-time clock chip and reset system; (d) The maliciously programmed ATtiny microcontroller

4.3 Validation of Security-Oriented PDN Modeling and Simulation Tool

We then validate PowerScout based on replicating the experiments in the literature [8], [16]–[18]. For the security perspective of PDN, the results show that PowerScout can correctly predict the performance of the attack. Further aided by PowerScout, we are able to perform nodal analysis and systemically evaluate the side-channel vulnerability under multiple PDN configurations. For example, we revel that removing near-chip capacitors can increase intra-chip information leakage by a maximum of 23.23dB at mid-frequency and inter-chip leakage by an average of 31.68dB at mid-and high-frequencies (as shown in Figure 10 (a)). And for inter-chip information leakage, near-chip capacitors increase information strength at both mid and high frequencies by an average of 31.68dB (as shown in Figure 10 (b)).

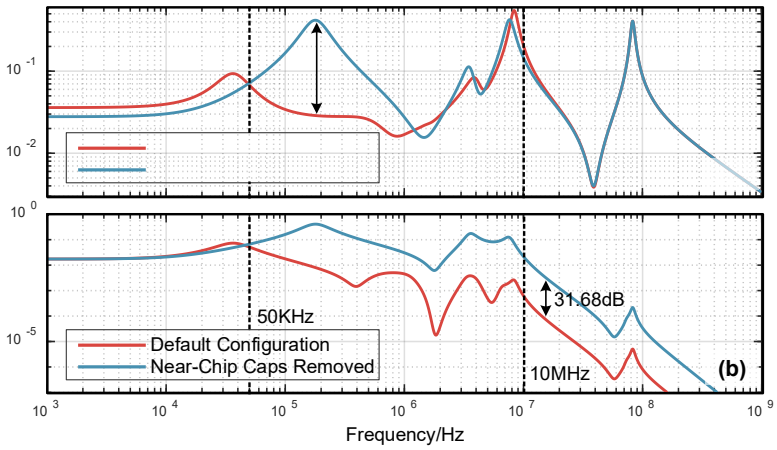

Figure 10 The information strength of (a) intra-chip and (b) inter-chip information leakage under two configurations.

Based on PowerScout, we also can find the features of PDN impedance profile (i.e., high-frequency part of impedance profile) that cannot be fully modeled by discrete components. The high frequency part of the PDN impedance is due to both board resonance and the discrete components. We further prove that due to the board resonance, the PDN is sensitive to the malicious modifications that negligibly impact PDN from a circuit perspective. As shown in Figure 11, we compare the impedance between the different booting configurations of the customized board. There are three configurations available: B0, B1, and B0+B1, since there are two booting configuration pins. Under each configuration, the corresponding pins (B0 and/or B1) are connected to the supply of the PDN to assign the pins a logic high. Since the jumper connects a high-impedance pin to the PDN, which cannot be detected from the circuit view due to the impedance of PDN is much smaller compared to the impedance of the pin. However, these three booting configurations greatly affect the board resonance and can be clearly recognized from the impedance changes at high frequency range. We are able to achieve 100% detection rate for detecting different configurations on customized boards.

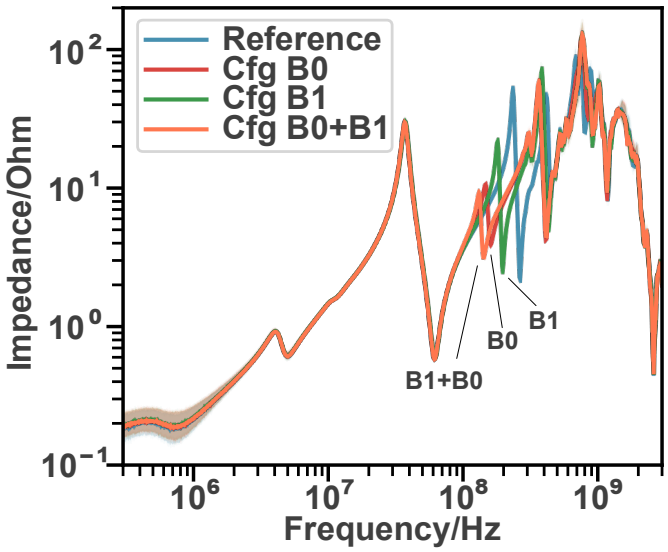

Figure 11 Proof-of-concept results of customized PCB showing PDN sensitivity for different board-level configurations.

5.0 CONCLUSIONS

Our results have proven that the proposed PDN-Pulse method can overcome the limitations of existing ad-hoc detection schemes. We have demonstrated two detection approaches using either network analyzer measurements when the suspect system is powered off (off-line) or spectrum analyzer measurements when the system if powered on (on-line). We can successfully detect and distinguish multiple types of anomalies such as power side-channel analysis attacks, malicious chip implants, in-filed hardware configuration tampers, and counterfeit PCB designs, as captured by our board-level attack benchmark. We achieved a 100% probability of detection (PD) and 0% probability of false alarm (PFA) on customized boards by correctly identifying Trojans existence among 36 samples, and achieved up to 93.75% PD and 0% PFA with 5 training samples and 31 testing samples on COTS products (i.e. Arduino Uno boards). In addition, the proof-of-concept experiments also illustrate that the PDN profile is much more sensitive to the system design than the process variation, further proving that PDN-Pulse methods has a high SNR. Our modeling tool and benchmarking method also prove instrumental in enabling an effective evaluation framework for PDN-based detection. Our framework exhibits excellent extensibility with broad coverage of anomalies that arise from modifications on discrete components and power planes/traces layout, and can further expand to provide impedance-based detection on all traces and signal nets of the system. Future improvement of scalability can be achieved through multi-point probing and golden-model-free detection.

Accomplishments: To the best of our knowledge, PDN-Pulse is the first method that unifies the monitoring and detection of anomaly at the full system level and across design layers. Our experimental platform that is based on rigorous testing on both custom boards and COTS products with statistically significant repeatability crucially establishes the viability and practicality of our approach. Our work has also been highly recognized by the research community, winning Best Paper Award at AsianHOST 2020 and Best Paper Nomination at ASP-DAC 2021.

6.0 REFERENCES

[1] J. Harrison, N. Asadizanjani, and M. Tehranipoor, "On malicious implants in PCBs throughout the supply chain," *Integration*, vol. 79, no. March, pp. 12–22, Jul. 2021, doi: 10.1016/j.vlsi.2021.03.002.

[2] P. Qiu, D. Wang, Y. Lyu, and G. Qu, "Voltjockey: Breaching trustzone by software-controlled voltage manipulation over multi-core frequencies," *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 195–209, 2019, doi: 10.1145/3319535.3354201.

[3] A. Tang, S. Sethumadhavan, and S. Stolfo, "CLKSCREW: Exposing the perils of security-oblivious energy management," *26th USENIX Secur. Symp. (USENIX Secur. 17)*, pp. 1057–1074, 2017, doi: 10.7916/d8-0ytv-3a53.

[4] L. N. Nguyen, C.-L. Cheng, F. T. Werner, M. Prvulovic, and A. Zajic, "A Comparison of Backscattering, EM, and Power Side-Channels and Their Performance in Detecting Software and Hardware Intrusions," *J. Hardw. Syst. Secur.*, no. Ic, Mar. 2020, doi: 10.1007/s41635-020-00093-y.

[5] S. K. Haider, C. Jin, M. Ahmad, D. M. Shila, O. Khan, and M. Van Dijk, "Advancing the state-of-the-art in hardware trojans detection," *IEEE Trans. Dependable Secur. Comput.*, vol. 16, no. 1, pp. 18–32, Jan. 2019, doi: 10.1109/TDSC.2017.2654352.

[6] J. Francq and F. Frick, "Introduction to Hardware Trojan Detection Methods," in *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2015*, May 2015, pp. 770–775, doi: 10.7873/DATE.2015.1101.

[7] M. Tehranipoor and F. Koushanfar, "A Survey of Hardware Trojan Taxonomy and Detection," *IEEE Des. Test Comput.*, vol. 27, no. 1, pp. 10–25, Jan. 2010, doi: 10.1109/MDT.2010.7.

[8] M. Zhao and G. E. Suh, "FPGA-Based Remote Power Side-Channel Attacks," in *2018 IEEE Symposium on Security and Privacy (SP)*, May 2018, vol. 2018-May, pp. 229–244, doi: 10.1109/SP.2018.00049.

[9] M. Kar, A. Singh, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Reducing power side-channel information leakage of AES engines using fully integrated inductive voltage regulator," *IEEE J. Solid-State Circuits*, vol. 53, no. 8, pp. 2399–2414, 2018, doi: 10.1109/JSSC.2018.2822691.

[10] D. Mahmoud, M. Stojilović, M. Stojilovi, and A. Adversary, "Timing Violation Induced Faults in Multi-Tenant FPGAs," *Proc. 2019 Des. Autom. Test Eur. Conf. Exhib. DATE 2019*, no. Section II, pp. 1724–1729, Mar. 2019, doi: 10.23919/DATE.2019.8715263.

[11] M. Lipp *et al.*, "PLATYPUS: Software-based Power Side-Channel Attacks on x86," in *IEEE Symposium on Security and Privacy (SP)*, 2021, [Online]. Available: https://publications.cispa.saarland/id/eprint/3357%0A.

[12] A. Zou *et al.*, "Ivory: Early-Stage Design Space Exploration Tool for Integrated Voltage Regulators," in *Proceedings of the 54th Annual Design Automation Conference 2017 on - DAC '17*, Sep. 2017, vol. 53, no. 9, pp. 1–6, doi: 10.1145/3061639.3062268.

[13] M. S. Gupta, J. L. Oatley, R. Joseph, G.-Y. Y. Wei, and D. M. Brooks, "Understanding Voltage Variations in Chip Multiprocessors using a Distributed Power-Delivery

Network," in *2007 Design, Automation & Test in Europe Conference & Exhibition*, Apr. 2007, vol. 1, no. January 2007, pp. 1–6, doi: 10.1109/DATE.2007.364663.

[14] J. Leng, Y. Zu, M. Rhu, M. Gupta, and V. J. Reddi, "GPUVolt: Modeling and Characterizing Voltage Noise in GPU Architectures," in *Proceedings of the 2014 international symposium on Low power electronics and design - ISLPED '14*, 2014, pp. 141–146, doi: 10.1145/2627369.2627605.

[15] A. Zou *et al.*, "Voltage-Stacked GPUs: A Control Theory Driven Cross-Layer Solution for Practical Voltage Stacking in GPUs," in *2018 51st Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*, Oct. 2018, vol. 2018-Octob, pp. 390–402, doi: 10.1109/MICRO.2018.00039.

[16] F. Schellenberg, D. R. E. Gnad, A. Moradi, and M. B. Tahoori, "An inside job: Remote power analysis attacks on FPGAs," in *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Mar. 2018, vol. 2018-Janua, pp. 1111–1116, doi: 10.23919/DATE.2018.8342177.

[17] D. R. E. E. Gnad, F. Oboril, and M. B. Tahoori, "Voltage drop-based fault attacks on FPGAs using valid bitstreams," in *2017 27th International Conference on Field Programmable Logic and Applications (FPL)*, Sep. 2017, pp. 1–7, doi: 10.23919/FPL.2017.8056840.

[18] J. Krautter, D. R. E. Gnad, and M. B. Tahoori, "FPGAhammer : Remote Voltage Fault Attacks on Shared FPGAs , suitable for DFA on AES," *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, vol. 2018, no. 3, pp. 44–68, 2018, doi: 10.13154/tches.v2018.i3.44-68.

APPENDIX A – PUBLICATIONS AND PRESENTATIONS

Presentation:

10/28/2020. Project Report of PDN-Pulse: Ubiquitous and Inherent Anomaly Detection with Cross-Layer Interactions of Power Delivery Network. Project Meeting with DARPA and AFRL sponsors. Xuan 'Silvia' Zhang, and Yier Jin.

12/15/2020-12/17/2020. PowerScout: A Security-Oriented Power Delivery Network Modeling Framework for Cross-Domain Side-Channel Analysis. IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST) Conference. Xuan 'Silvia' Zhang, Yier Jin, and Huifeng Zhu.

1/18/2021-1/21/2021. PCBench: Benchmarking of Board-Level Hardware Attacks and Trojans. 26th Asia and South Pacific Design Automation Conference (ASP-DAC). Xuan 'Silvia' Zhang, Yier Jin, and Huifeng Zhu.

2/16/2021. Project Report of PDN-Pulse: Ubiquitous and Inherent Anomaly Detection with Cross-Layer Interactions of Power Delivery Network. Project Meeting with DARPA and AFRL sponsors. Xuan 'Silvia' Zhang, and Yier Jin.

Publication:

PowerScout: A Security-Oriented Power Delivery Network Modeling Framework for Cross-Domain Side-Channel Analysis. Huifeng Zhu, Xiaolong Guo, Yier Jin, Xuan Zhang. IEEE Asian Hardware Oriented Security and Trust Symposium (AsianHOST). 12/2020.

PCBench: Benchmarking of Board-Level Hardware Attacks and Trojans. Huifeng Zhu, Xiaolong Guo, Yier Jin, and Xuan Zhang. 26th Asia and South Pacific Design Automation Conference (ASP-DAC).

LIST OF SYMBOLS, ABBREVIATIONS, AND ACRONYMS

PDN	Power Delivery Network
COTS	Commercial-off-the-shelf
SoC	System-on-Chip
PCB	Printed Circuit Board
FPGA	Field Programmable Gate Array
VRM	Voltage Regulator Module
RLC	Resistor-Inductor-Capacitor
SMA	Subminiature version A
VNA	Vector Network Analyzer
MCU	Microcontroller
CPA	Correlation Power Analysis
DPA	Differential Power Analysis
EM	Electromagnetic
PD	Possibility of Detection
PFA	Possibility of False Alarm
I/O	Input/Output
C4	Controlled Collapse Chip Connection
ESL	Equivalent Series Inductor
ESR	Equivalent Series Capacitor
VDD	Power Supply
GND	Ground
LDO	Low-dropout Regulators