Research Statement

Patanjali Sristi

1 Overview

We live in a connected world. Today's devices are no longer monolithic entities but comprise several moving parts at various abstractions, such as software, OS, Kernel, and hardware interacting seamlessly to perform complex tasks. From a security standpoint, this is interesting since the system's overall integrity relies on all these components being trustworthy. My research focuses on answering the question: **"How to achieve affordable security assurances given an untrusted ecosystem consisting of multiple interacting components while adhering to the constraints on resources at each abstraction such as storage, computation, and energy available for these devices?"** Such themes are instrumental in IoT, AI applications and even in data centers where the resources allocated for security are minimal. In this context, I have so far looked at some of the security issues in networking protocols, IoT platforms, and the manufacturing of hardware devices. Beyond this, I have also looked at the security of systems (that includes networks and standalone systems) that are assembled from individual components purchased from different vendors. Therefore, my research is multi-disciplinary, often straddling across the domains of computer networking, computer architecture, and VLSI design.

2 Intellectual Merit and Impact

My research has led to **17 peer-reviewed journal and conference articles** [1–17]. I have published in some of the most competitive venues, such as the International Conference on Computer-Aided Design (ICCAD), Design Automation and Test Conference in Europe (DATE), IEEE Transactions on Very Large Scale Integrated Systems (TVLSI), and IEEE Transactions on Computers. I have **6 US patents** filed [18–23] for different inventions in domains such as SoC security and the Internet of Things. I also have **6 works** [24–29] under various stages of review. My research work has been accepted for **SIGDA Ph.D. forum**. I have won several awards in various cybersecurity competitions across the world, including the **Winner** in Embedded Systems Security Challenge in Cybersecurity Awareness Week (CSAW) 2016 conducted by NYU, **Winner and Runner-up** in the Applied Research competition in CSAW 2020, **Runner-up** in the Best Student Demo in 1^{st} NELMS Annual IoT Conference in 2019. My research has also been featured in several reputed cybersecurity magazines such as **WIRED** [30], and BusinessInsider [31].

3 Collaboration with Industry and Government Research

During my Ph.D. and postdoc career, I was fortunate to collaborate with industry and research labs on interesting problems. During my Ph.D. tenure, I worked on the initial development of the Shakti microprocessor. I worked with two graduate students designing the Memory Management Unit for the Shakti microprocessor. This project was in collaboration with DRDO (Defence Research and Development Organization) and CDAC (Centre for Development of Advanced Computing), India. During my tenure as a postdoc at the University of Florida, I focused on extending my security expertise to designing secure IoT devices and developing System-on-Chip policies for securing the design from supply chain and in-field attacks through collaborations with industry groups such as Northrup Grumman (NG) and Intel.

4 Research Highlights

4.1 Hardware Security and Trust

I have worked on several research problems related to hardware security and have developed various solutions for combating semiconductor supply chain threats [8, 10].

4.1.1 Hardware Obfuscation

With my collaborators, I have worked on problems related to logic locking [16, 17], resulting in two publications and a journal article currently under review [29]. In both these research works, we ensured that our solution was implemented

on large-scale designs and evaluated using industry-standard toolchains and state-of-the-art attacks. In **IOLOCK** [17,29], we propose a design-level framework for preventing the attacker from gaining unauthorized access to a given design's Input/Output ports. We implement the framework on a MAX10 FPGA board and show that IOLOCK is resistant to every state-of-the-art attack in Logic Locking. Similarly, in **RIPPER** [16], we propose a logic redaction technique that removes some of the design logic and replaces it with a programmable fabric. Doing so would prevent Reverse-Engineering attacks at the cost of increased area. We modified the state-of-the-art FPGA mapping algorithm and showed that it is possible to incorporate the programmable fabric without incurring significant area overheads.

4.1.2 Hardware Trojan Detection and Resilience

Malicious design modifications or Trojans remain a pertinent threat to the Hardware ecosystem. Traditional Trojan detection techniques require the presence of a golden design for reference. However, this assumption is tricky when considering COTS (Commercial of the Shelf) components typically procured from third-party vendors and then integrated. This is usually the case in the Internet of Things (IoT) and Edge devices. With my collaborators, I have developed an ML-based technique that can detect Trojans without using a reference design [13]. In this work, we use a K-Means clustering approach that uses Side-channel Signatures to detect malicious modifications. This work was accepted as a conference submission in *International Symposium on Quality Electronic Design (ISQED)*. We have also developed a metric titled **Trojan Vulnerability Factor** (TVF) for estimating the susceptibility of a design towards Trojan insertion [28]. Typical metrics assess vulnerability as a function of the number of suspect nets in the design, which requires an analysis of the entire design. This is cumbersome for larger designs. In our work, we map the effort of inserting Trojans to the maximal clique analysis problem in Graph theory and propose TVF, a metric that quantifies the vulnerability of a given design against Trojan insertion. With such analysis, we can frame the threat to represent the Trojan behavior more accurately and quantify the effort required for a designer to cover these Trojans. TVF is currently under review as a regular article in *IEEE Transactions on Very Large Scale Integrated Systems (TVLSI)*.

4.1.3 Side-channel Attacks and Defenses

Hardware is the root of trust for many security solutions. However, in recent times, attackers have exposed multiple vulnerabilities, asserting that their security cannot be taken for granted. Most of the recent attacks leverage the timing or the power side channel that leaks information about the computation being performed by the CPU. In **Karna** [6], we propose an Electronic Design Automation (EDA) plug-in that the hardware designers can use to ensure that the manufactured chip does not have any power side channel. Karna does not add any new logic gates but only reorganizes and reconfigures the existing logic gates to prevent side-channel leakage. The ability of Karna to do so with absolutely no increase in area, power, and delay of the chip was appreciated by the research community. Karna has been published as a poster and a paper at the *Design Automation Conference (DAC)* and *International Conference on Computer-Aided Design (ICCAD)*, respectively. We have extended the observations in Karna to develop a tool called **SOLOMON** that can identify locations in the design susceptible to Fault Attacks [5] and developed a framework called **Avatar** [14] that reconfigures the gates in the design to prevent Fault attacks. Solomon was accepted in the *Design Automation and Test Conference in Europe (DATE)*, while Avatar has been accepted in *Asia and South Pacific Design Automation Conference (ASP-DAC)*.

4.2 Embedded Systems Security

Embedded systems present an interesting challenge from a security viewpoint. These devices often operate under heavily resource-constrained settings and thus cannot support the additional infrastructure, such as extra hardware or software modules needed to guarantee trustworthiness. However, they also have access to sensitive user data in most applications and thus need to be secured.

4.2.1 Hardware software co-design for preventing embedded systems security

We explored the problem of securing embedded devices from memory corruption attacks in our work **Gandalf** [2]. Existing software-only defense schemes have unreasonable overheads, while the hardware-only methods cannot boot the Linux kernel without significant modifications to the software stack. Gandalf has low overheads, while at the same time, it is also capable of booting the vanilla Linux kernel. Our initial results were published in *IEEE Embedded systems letters(ESL)*. We also identified vulnerabilities in state-of-the-art timing side-channel defense called CAESAR and proposed a lightweight countermeasure called **Brutus** [7] published in *IEEE Computer Architecture Letters(CAL)*. Gandalf and Brutus have been integrated into the indigenous microprocessor of India, named Shakti.

4.2.2 Lightweight security protocols for Embedded Systems

Another exciting research avenue I explored with my collaborators is the problem of developing security protocols for Embedded Systems. Embedded devices have a widely distributed supply chain, with most components procured via third-party vendors or resellers. Thus the issues of piracy, counterfeiting, and malicious devices that plague the traditional IC supply chain only become exacerbated. However, conventional methods for preventing such attacks require additional hardware that incurs significant area and power overheads. We developed lightweight authentication protocols that can be utilized for Edge and IoT-scale devices. We developed a Physically Unclonable Function called **MeLPUF** that the designer can integrate into the design seamlessly and show that MeLPUF incurs lesser area and power overheads while providing strong security guarantees [24]. We also developed a lightweight watermarking protocol called **SIGNED** [11] that can also be incorporated into designs with minimal overheads and show that it is resistant to tampering, modification, and removal attacks. MeLPUF is currently under review in the *ACM Journal of Emerging Technologies (JETC)*, while SIGNED has been accepted as a regular article in *IEEE Transactions on Computers (TC)*.

4.3 Network Security

During my Ph.D., I had a chance to work with my collaborators on research problems that focused on identifying network-level side channels. Our work titled **White Mirror** analyzes the network traffic to identify information leakage even when the packets are encrypted. The first work showed that it was possible to infer the user choices when watching an interactive movie such as "Black Mirror: Bandersnatch " [4]. Our privacy measurement study was accepted as a submission in *ACM SIGCOMM* and was also featured in **WIRED** Magazine [30]. The subsequent work showed that even when using security-centric network protocols, the performance constraints would still enable the attacker to eavesdrop and infer sensitive information [9] which was accepted as a conference submission in *IEEE/IFIP International Conference on Dependable Systems and Networks.*

5 Future Research Directions

5.1 Hardware Security

I want to work with students and faculty to extend my current research on hardware security, focusing on side-channel attacks and defenses and developing novel metrics to quantify the trustworthiness of a given design against various supply chain attacks. My research would also focus on identifying new vulnerabilities in the supply chain/deployment ecosystem at the software/hardware/network level.

5.2 Methodology and Tool-flow for Secure System-on-Chip (SoC) Architectures

SoC architectures consist of several IPs, each with its own performance, interoperability, and security constraints. The complexity in SoC trust assurance arises due to the following factors; the diverse trust requirements imply that each IP in the design could have a different security countermeasure. Thus the problem of securing the SoC becomes twofold: i) identifying the optimal security countermeasure that can meet the performance and interoperability constraints of the IP and the overall SoC. ii) ensure that these security countermeasures are integrated such that the security of the other IPs and, consequently, the overall SoC is not impacted. Additionally, modern SoCs have different architectures, such as Network-on-Chip (NoCs), 3DICs etc., to address the area and power constraints. Thus, any security solution must be adaptable to these non-traditional architectures. I have developed solutions for SoC security [25–27] and would be extending these solutions to address other security issues in SoC architectures.

5.3 AI-guided techniques for VLSI Design Automation

Modern VLSI designs require millions of gates to be synthesized, placed, routed, and the layout is generated under stringent performance constraints. The shrinking technology nodes and the shorter turnaround time further complicate this process. AI techniques have shown tremendous promise in tackling this challenge. I wish to build upon my previous efforts in designing energy efficient systems [1, 3] using Machine Learning to develop novel algorithms for identifying and addressing various issues in VLSI Design Automation.

5.4 Hardware/Software co-design for secure embedded systems

I wish to explore research problems related to the security of Embedded/Edge devices and work toward identifying novel attack vectors in various deployment scenarios. I would also work with students to develop design-level countermeasures to develop frameworks for detecting and preventing security vulnerabilities such as malware, denial-of-service attacks, etc.

6 Potential Collaboration and Funding Sources

In Summary, my goal is to focus on building state-of-the-art technologies for addressing various research challenges in cybersecurity. I would leverage the knowledge and expertise I gained during my Ph.D. and postdoc career. I also want to simultaneously learn and expand my research interests by collaborating with other faculty, especially in AI and IoT domains, to build safe, secure, and energy-efficient systems that can be deployed to make our daily lives better. I have gained valuable experiences in working with faculty both in IIT Madras and the University of Florida to write proposals for research labs such as DARPA, Sandia Labs, and Northrup Grumman, as well as industry agencies such as Microsoft and Intel. This experience will be beneficial in writing funding proposals to different agencies at the beginning of my professional career. I sincerely look forward to beginning my career as a faculty member and researcher in these important and promising areas.

References

[1] A. Gautham, K. Korgaonkar, P. Slpsk, S. Balachandran, and K. Veezhinathan, "The implications of shared data synchronization techniques on {Multi-Core} energy {Efficiency}," in *2012 Workshop on Power-Aware Computing and Systems (HotPower 12)*, 2012.

[2] G. Krishnakumar, P. SLPSK, P. K. Vairam, C. Rebeiro, and K. Veezhinathan, "Gandalf: A fine-grained hardware–software co-design for preventing memory attacks," *IEEE Embedded Systems Letters*, vol. 10, no. 3, pp. 83–86, 2018.

[3] S. Patanjali, M. Patnaik, S. Potluri, and V. Kamakoti, "Mltimer: Leakage power minimization in digital circuits using machine learning and adaptive lazy timing analysis," *Journal of Low Power Electronics*, vol. 14, no. 2, pp. 285–301, 2018.

[4] G. Mitra, P. K. Vairam, P. Slpsk, and N. Chandrachoodan, "White mirror: Leaking sensitive information from interactive netflix movies using encrypted traffic analysis," in *Proceedings of the ACM SIGCOMM 2019 Conference Posters and Demos*, 2019, pp. 122–124.

[5] M. Srivastava, P. Slpsk, I. Roy, C. Rebeiro, A. Hazra, and S. Bhunia, "Solomon: An automated framework for detecting fault attack vulnerabilities in hardware," in *2020 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2020, pp. 310–313.

[6] P. Slpsk, P. K. Vairam, C. Rebeiro, and V. Kamakoti, "Karna: A gate-sizing based security aware eda flow for improved power side-channel attack protection," in *2019 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. IEEE, 2019, pp. 1–8.

[7] R. Bodduna, V. Ganesan, P. Slpsk, K. Veezhinathan, and C. Rebeiro, "Brutus: Refuting the security claims of the cache timing randomization countermeasure proposed in ceaser," *IEEE Computer Architecture Letters*, vol. 19, no. 1, pp. 9–12, 2020.

[8] T. Hoque, P. Slpsk, and S. Bhunia, "Trust issues in microelectronics: The concerns and the countermeasures," *IEEE Consumer Electronics Magazine*, vol. 9, no. 6, pp. 72–83, 2020.

[9] G. Mitra, P. K. Vairam, P. Slpsk, N. Chandrachoodan, and V. Kamakoti, "Depending on http/2 for privacy? good luck!" in *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. IEEE, 2020, pp. 278–285.

[10] T. Hoque, P. SLPSK, and S. Bhunia, "Trust issues in cots: The challenges and emerging solution," in *Proceedings of the 2020 on Great Lakes Symposium on VLSI*, 2020, pp. 211–216.

[11] P. SLPSK, A. A. Nair, C. Rebeiro, and S. Bhunia, "Signed: A challenge-response scheme for electronic hardware watermarking," *IEEE Transactions on Computers*, 2022.

[12] F. Zhang, S. D. Paul, P. Slpsk, A. R. Trivedi, and S. Bhunia, "On database-free authentication of microelectronic components," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 29, no. 1, pp. 149–161, 2020.

[13] S. Yang, P. Chakraborty, P. SLPSK, and S. Bhunia, "Trusted electronic systems with untrusted cots," in *2021 22nd International Symposium on Quality Electronic Design (ISQED)*. IEEE, 2021, pp. 198–203.

[14] P. B. Roy, P. Slpsk, and C. Rebeiro, "Avatar: Reinforcing fault attack countermeasures in eda with fault transformations," in *2022 27th Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE, 2022, pp. 417–422.

[15] S. D. Paul, F. Zhang, P. SLPSK, A. R. Trivedi, and S. Bhunia, "Rihann: Remote iot hardware authentication with intrinsic identifiers," *IEEE Internet of Things Journal*, vol. 9, no. 24, pp. 24 615–24 627, 2022.

[16] A. Dasgupta, M. M. Rahman, P. SLPSK, N. Dorairaj, D. Kehlet, and S. Bhunia, "Ripper 2.0: A novel attack-resistant optimization methodology for hardware redaction," *GOMACTech*, 2023.

[17] C. Vega, P. SLPSK, and S. Bhunia, "Iolock: An input/output locking scheme for chip and pcb protection," *GOMACTech*, 2023.

[18] P. Chakraborty, R. Dizon, C. Vega, J. B. Harley, S. Ray, S. Bhunia, and S. L. S. Patanjali, "Smart infrastructures and first-responder network for security and safety hazards," Feb. 10 2022, uS Patent App. 17/392,376.

[19] S. B Bhunia, P. Chakraborty, R. Dizor, P. Difuntorum, C. Vega, and S. L. S. Patanjali, "Drone-based administration of remotely located instruments and gadgets," Mar. 17 2022, uS Patent US20220083987A1.

[20] S. Bhunia, C. Vega, R. Dizon, R. R. Kalavakonda, and S. L. S. Patanjali, "Reconfigurable jtag architecture for implementation of programmable hardware security features in digital designs," Nov. 10 2022, uS Patent 20,220,357,394.

[21] S. Bhunia, T. Hoque, A. A. Nair, and S. L. S. Patanjali, "Framework for obfuscation based watermarking," Oct. 14 2021, uS Patent App. 17/224,559.

[22] S. Bhunia, C. Vega, S. D. Paul, P. Difuntorum, R. Dizon, and S. L. S. Patanjali, "Defense of jtag i/o network," Dec. 16 2021, uS Patent App. 17/303,648.

[23] S. Bhunia, P. Deb, N. Atul, K. Raj, S. Ray, and S. L. S. Patanjali, "Establishing trust in untrusted ic testing and provisioning environment," Nov. 24 2022, uS Patent App. 17/662,399.

[24] C. Vega, P. SLPSK, S. D. Paul, and S. Bhunia, "Melpuf: Memory in logic puf," *ACM Journal on Emerging Technologies in Computing Systems*, 2023.

[25] P. SLPSK, M. M. Rahman, J. Cruz, , and S. Bhunia, "SOLO: A novel distributed locking protocol for securing system on chip architectures," *IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems (TCAD)*, 2023.

[26] P. SLPSK, J. Cruz, S. Ray, and S. Bhunia, "Protects:a framework for secure provisioning of system-on-chip assets in untrusted testing facility," *ACM Design Automation Conference*, 2023.

[27] P. SLPSK, S. Ray, and S. Bhunia, "Treehouse: A secure asset management infrastructure for protecting 3dic design," *IEEE Transactions on Computers*, 2023.

[28] J. Cruz, P. SLPSK, P. Gaikwad, and S. Bhunia, "Tvf: A metric for quantifying vulnerability against hardware trojan attack," *IEEE Transactions on Very Large Scale Integrated Systems(TVLSI)*, 2023.

[29] C. Vega, P. SLPSK, and S. Bhunia, "Iolock: An input/output locking scheme for chip and pcb protection against reverse-engineering attacks," *IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems (TCAD)*, 2023.

[30] C. Nast, "Hackers Can Tell What Netflix Bandersnatch Choices You Make," https://www.wired.com/story/netflix-interactive-bandersnatch-hackers-choices/, [Accessed 15-Dec-2022].

[31] "Meet the IITians who have made their way into world's largest hardware hacking competition finals," https://www.businessinsider.in/meet-the-iitians-who-have-made-their-way-into-worlds-largest-hardware-hacking-competition-finals/articleshow/54831499.cms, [Accessed 15-Dec-2022].