Jubayer Mahmod

Senior Engineer, Offensive security @ Lucid Motors, CA
Hardware Security PhD @ Virginia Tech

https://computing.ece.vt.edu/∼Jubayer/
jubayer@vt.edu
+1 (334) 524-6872
https://www.linkedin.com/in/jubayer0175/

Research Interests

With 6+ years of experience in hardware-oriented system security, my expertise encompasses a wide range of interests, including the security of systems, firmware, and hardware. My doctoral research is centered on leveraging architectural and low-level hardware behaviors to develop system-level attack and defense strategies. This includes work on trusted execution environments, side-channel attacks, cloud FPGA security, and the creation of innovative frameworks for anti-counterfeit chip detection and avoidance.

Education

PhD, Computer Engineering, Virginia Tech, USA 08/19–04/24
Thesis: The Art of SRAM Security: **Advisor:**Dr. Matthew Hicks
Tactics for Remanence-based Attack and Strategies for Defense

MS, Electrical & Computer Engineering, Auburn University, AL, USA 08/17–08/19
Thesis: Towards Unclonable System Design for Resource-Constrained Applications **Advisor**: Dr. Ujjwal Guin

BS, Electrical & Electronic Engineering (EEE) 03/16
Bangladesh University of Engineering & Technology (BUET), Dhaka
Thesis: Metal-Insulator-Metal Ring Resonator Design for Sensing Applications **Advisor:** Dr. Zahurul Islam

Experience & Internships

Lucid Motors, CA	Senior Security Engineer	04/24– now
Virginia Tech, VA	Graduate Research Assistant	01/20– 04/24
ForteMedia, Inc, Santa Clara, CA	Graduate Engineering Intern	Summer 2018, 2019
Auburn University, AL	Graduate Research Assistant	08/17 - 05/19

Research Summary

First authored publications in top-tier venues (3): Oakland(x1), ASPLOS(x2)
Other publications (6)

Selected Publications

1. **Jubayer Mahmod** & Matthew Hicks. *UnTrustZone: Systematic Accelerated Aging to Expose On-chip Secrets.* IEEE Symposium on Security and Privacy 2024 (Acceptance rate: 17.8%).
2. **Jubayer Mahmod** & Matthew Hicks. *SRAM Imprinting for System Protection and Differentiation.* The 19th ACM ASIA Conference on Computer and Communications Security (To appear in ACM ASIACCS 2024)(Acceptance rate: 19%).
3. **Jubayer Mahmod** & Matthew Hicks. *Invisible Bits: Hiding Secret Messages in SRAM's Analog Domain.* International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS'22), (Acceptance rate: 20%)
4. **Jubayer Mahmod** & Matthew Hicks. *SRAM Has No Chill: Exploiting Power Domain Separation to Steal Onchip Secrets.* International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS'22), (Acceptance rate: 20%).
5. **Jubayer Mahmod** & Matthew Hicks. *Retain The Date: Purging Recycled Chips from the Supply Chain through SRAM's Data Retention Behavior (under submission)*
6. **Jubayer Mahmod** & Ujjwal Guin. *A Robust, Low-Cost and Secure Authentication Scheme for IoT Applications*. Cryptography 4.1 (2020)
7. **Jubayer Mahmod**, Millican Spencer, Ujjawal Guin, and Vishwani Agrawal. *Delay Fault Testing: Present and Future*. IEEE VLSI Test Symposium (VTS'19).
8. Benjamin Cyr, **Jubayer Mahmod**, Ujjwal Guin. *Low-Cost and Secure Firmware Obfuscation Method for Protecting Electronic Systems from Cloning*. IEEE Internet of Things Journal (2019)

Teaching Experience

Virginia Tech	ECE 4514: Digital Design II	GTA	Fall 2019
Auburn University	ELEC 6970: Hardware Security I	GTA	Fall 2018
Daffodil International University, Dhaka	Undergraduate electronics courses	Lecturer	09/16-07/17

TECHNICAL SKILLS

• Hardware/software co-design • Applied Cryptography • ARM SoC/Cloud FPGA security (aws F1)
• TEE: ARM TrustZone, SGX • Linux kernel, Coreboot, secure debug, Threat modeling
• C, Assembly (x86 & ARM), Verilog, Python • Cadence Design Tools, Hspice.

SELECTED PROJECTS

- **Exploiting SRAM data remanence to design attacks**: Leveraged SRAM's analog characteristics and power domain separation to design **Volt Boot** and **UntrustZone**. Volt Boot shows how to create artificial data retention across power cycles in an SoC 100% accuracy. Using a secure boot or a trusted execution environment can be potential mitigation, which inspired a more robust form of attack on ARM TrustZone—UntrustZone—that still exfiltrates data/code ($> 98\%$ accuracy) from on-chip SRAM using accelerated transistor wear-out. **Outcome**: two top-tier conference publications.
- **Defenses leveraging SRAM data remanence**: Designed data hiding & SoC anti-counterfeit systems utilizing SRAM's analog behavior, specifically circuit aging. **Invisible bits** is a steganography scheme that creates a covert, cryptographically secure but plausibly deniable information transfer channel in the hardware. Further applied imprinting and data retention voltage techniques for detecting and avoiding recycled, remarked, and cloned chips. **Outcome**: Three papers [Invisible bits, Retain-the-date, SKU-RAM]
- **Cloud FPGA localization**: Developed a cloud FPGA localization system using dynamic timing faults in functionally valid circuits, circumventing AWS security restrictions on hardware DNA access. This entirely **on-chip** signature extraction method achieves >**99% accuracy**, **operates 13X faster**, and **costs 92% less** than the state-of-the-art (under review).
- **Hardware-assisted firmware obfuscation**: Developed a custom MIPS core featuring a reorder cache in the instruction fetch unit, enabling dynamic and transparent reconstruction of control flow from obfuscated firmware. **Outcome**: a journal paper.

Graduate course projects

- **Hardware/Software Co-Design**:
  – Machine learning inference: Developed a NIOS-II-based ML accelerator, focusing on resource-efficient heterogeneous computing through custom instruction & hardware/software co-design. Achieved **2500x** speed boost compared to baseline software-only implementation using ARM-FPGA system.
  – Crypto acceleration engines: Implemented RSA hardware engine using Radix-2 Montgomery multiplication and Chinese remainder theorem. AES Engine: Crafted for Hardware Trojan demonstrations.
- **Linux kernel programming**:
  – Intra-Process isolation: Utilized Intel's *Memory Protection Key (MPK)* and *libmpk* to explore user-space memory permission control at page granularity.
  – Distributed shared memory synchronization: Implemented MESI protocol to synchronize shared pages across multiple Linux processes/machines using user-space page-fault handling (user-faultfd).

PRESENTATION & TALKS

Exploring Dual Edges of SRAM Data Remanence in SoCs: Covert Storage and Exfiltration Risks in TEE (Hardwear.io)	2024
UnTrustZone: Systematic Accelerated Aging to Expose On-chip Secrets. (Oakland)	2024
Invisible Bits: Hiding Secret Messages in SRAM's Analog Domain. (ASPLOS)	2022
SRAM Has No Chill: Exploiting Power Domain Separation to Steal Onchip Secrets. (ASPLOS)	2022
SRAM PUF-based device authentication protocol hardware demo. (HOST)	2019
Graduate Research Showcasing. Auburn University	2018
Hardware Trojan showcasing (hardware & poster) NAE Grand Challenges Scholars Program	2018

AWARDS

PhD Dissertation finalist (1/5)	Symposium on Hardware Oriented Security & Trust	2024
NSF travel grant	ASPLOS, Switzerland	2022
NSF travel grant	Symposium on Hardware Oriented Security & Trust	2019
Graduate school tuition fellowship	Auburn University	2017-19
Best project award	Tensilica Xtensa Embedded-DSP design contest, India	2016
Dean's List award	BUET	

SERVICE

Reviewer:

– ICCD 2024
– Journal of Hardware and Systems Security 2023
– IEEE Internet of Things Journal 2022

External Reviewer:

• ASPLOS'24 • IEEE Transactions on Circuits and Systems I'21 • VLSID'19 • DAC'19 • GLSVLSI'19 • Journal of Hardware and Systems Security'19 • IEEE Transactions on Very Large Scale Integration Systems'17 &'18 • VLSI Test Symposium'18 • Transactions on Multi-Scale Computing Systems'18