Hardware/ Software Codesign Research at Georgia Tech

Vincent John Mooney III

Associate Professor, School of Electrical and Computer Engineering, Georgia Institute of Technology, Georgia, USA

Adjunct Associate Professor, School of Computer Science, Georgia Institute of Technology, Georgia, USA

Director, on-campus Master of Science in Cybersecurity (Cyber-Physical Systems track), Georgia Institute of Technology, Georgia, USA

http://mooney.gatech.edu

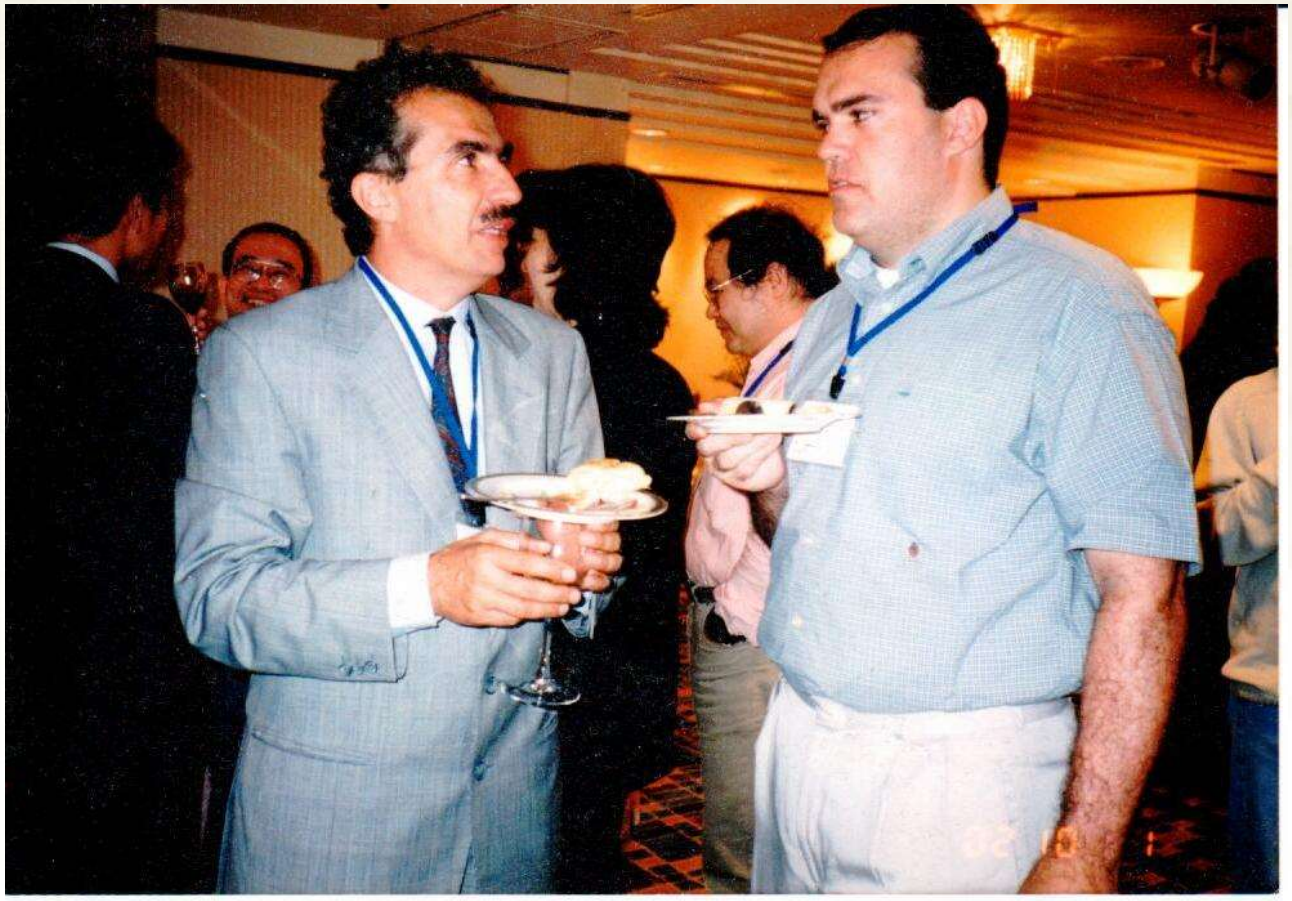
23 June 2024

Georgia Tech Institute for Information Security & Privacy

Master of Arts in Philosophy, 1997

- B.S. in E.E. and C.S., Yale U., 1991
- Certificate of Graduate Students, U. Navarra, Spain, 1992
- M.S. in E.E., 1994
- Polly told me she earned two M.S. degrees!
- M.A. in Philosophy, Symbolic Sys., 1997
- Ph.D. in E.E., 1998

CODES-ISSS Early 2000s



Adopted Family, 2006

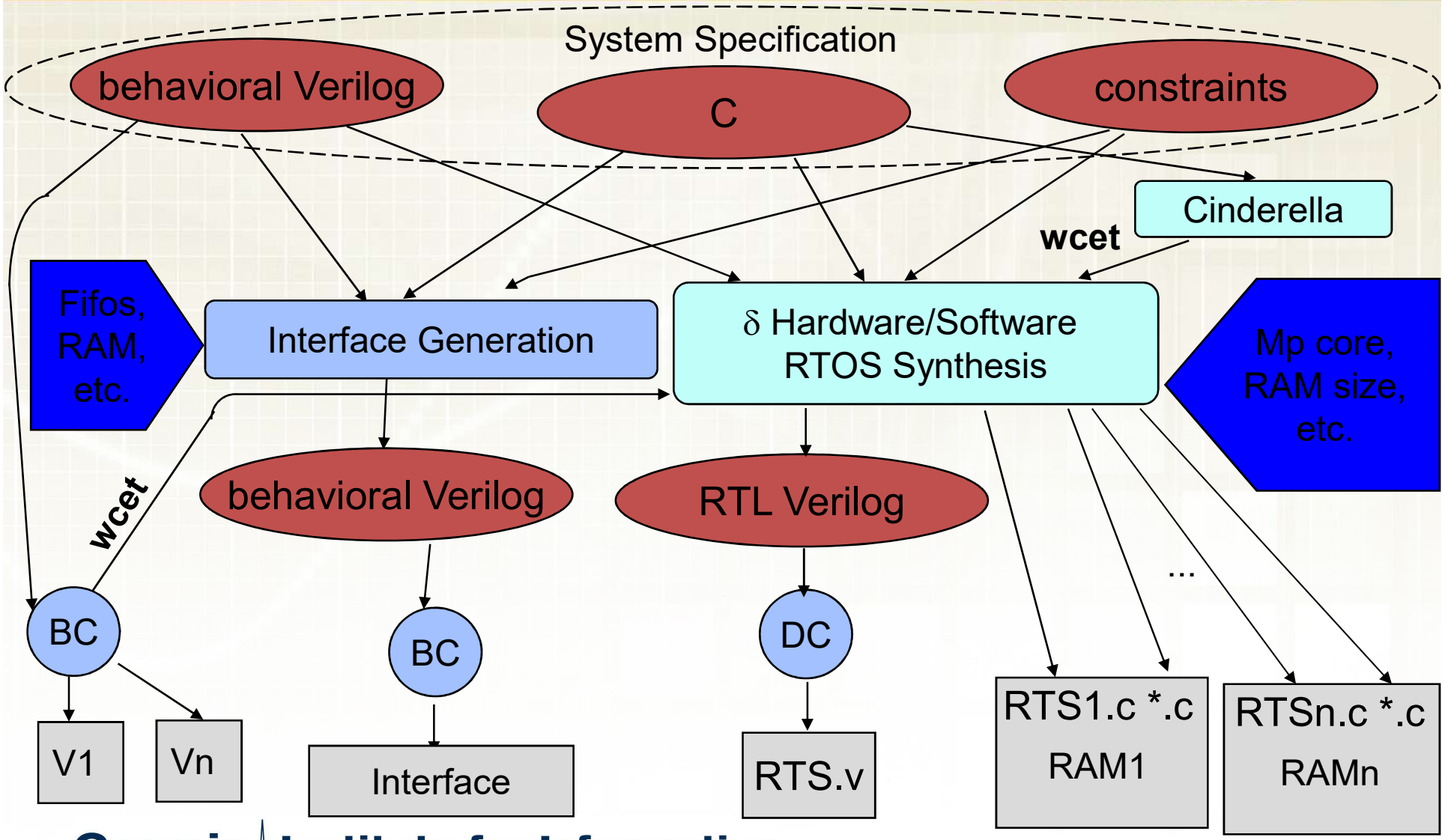
Past Ph.D. Theses Supervised

Remote Sensor Security Through Encoded Computation and Cryptographic Signatures
Cyber Threat Propagation Modeling in Cyber Physical Systems
Embedded Software Streaming
Medical Device Security Through Hardware Signatures
Assembly Instruction Level Reverse Execution for Debugging
Hw/Sw Deadlock Avoidance for Multiproc. Multiresource SoC
Cache Timing Analysis for Multi-tasking Real-Time Uniproc. Sys.
Dynamic Memory Management for Real-Time Multiprocessor SoC
The System-on-a-Chip Lock Cache
Automated Bus Generation for Multiprocessor System-on-a-Chip
Automated Generation of Round-robin Arb. & Xbar Switch Logic
Sleepy Stack: A New Approach to Low Power VLSI and Memory

Undergraduate Research

- Vertically Integrated Projects (VIP)
  - Provides one or two research credits per semester for up to three years
  - Integrated into the undergraduate degree
  - Approximately 10 students per semester over the past decade
- Recent achievement: Best Paper Award at MECO 2024, “Linguistic Encryption for Underwater Communication,” by 5 under-graduate students (**no** grad students)

SoC Programming Flow



HW/SW Codesign of an RTOS

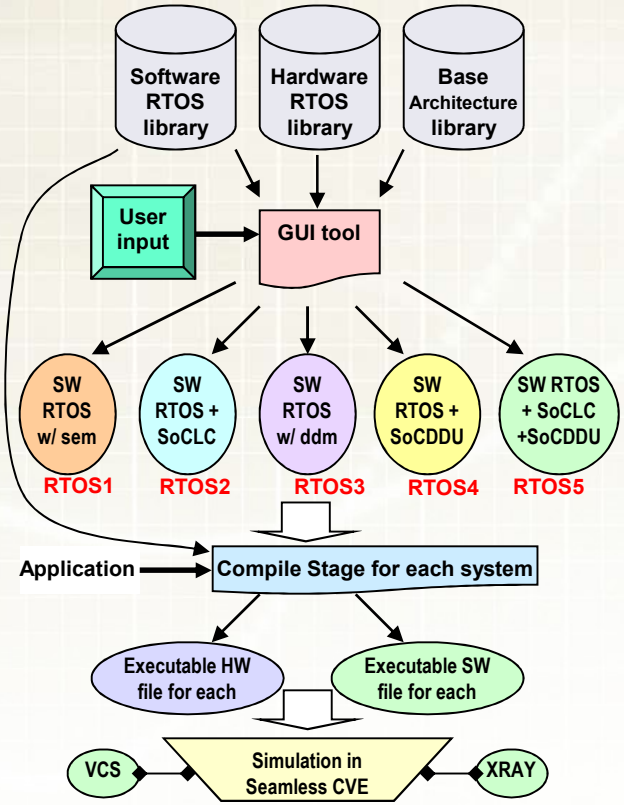


Figure 1: Five custom hardware/software RTOS Examples and Simulation

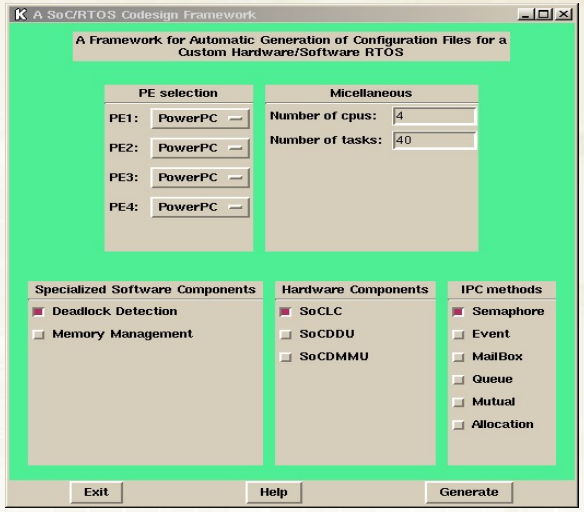


Figure 2: Graphical User Interface for the δ Framework

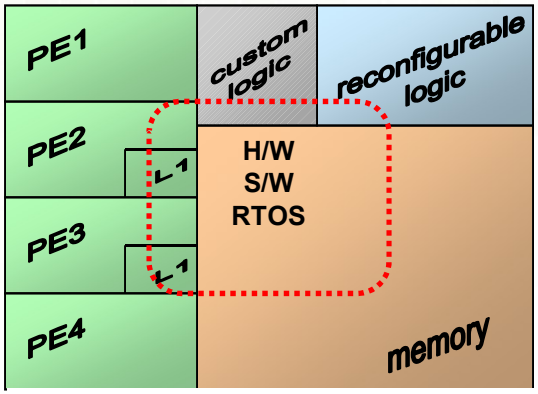
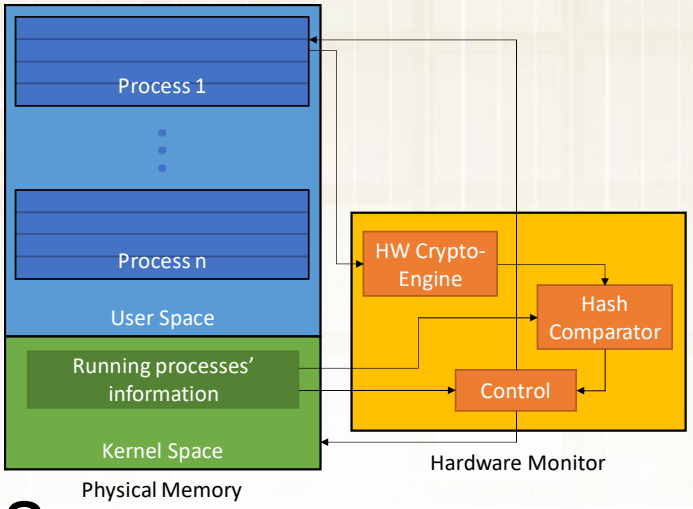


Figure 3: Sample SoC Architecture

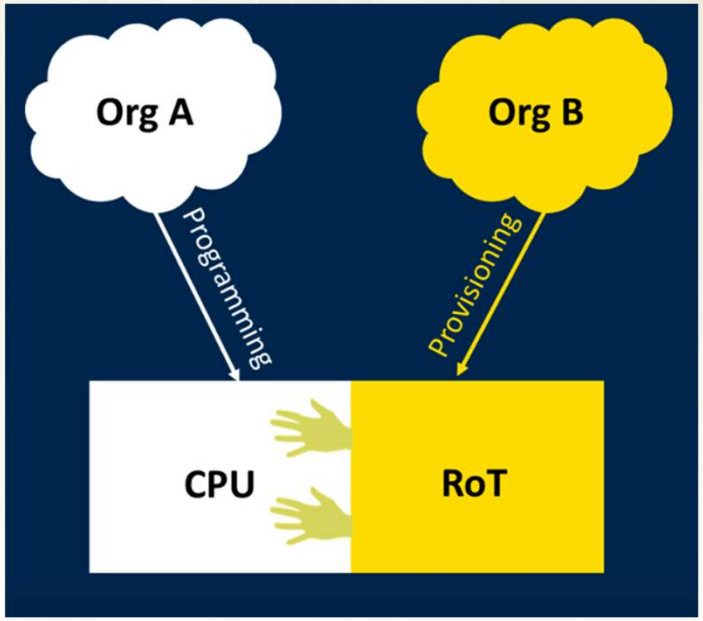
ECE 3170 Cryptographic Hardware

- Data Encryption Standard
- MD5
- Authentication protocols
- Oracle attacks
- Hiding and masking
- Differential Power Analysis



ECE 4823 / 8803 Hardware Security

- AES
- SHA2
- PUFs
- PUF-based authentication
- Hardware Trojans
- Meltdown

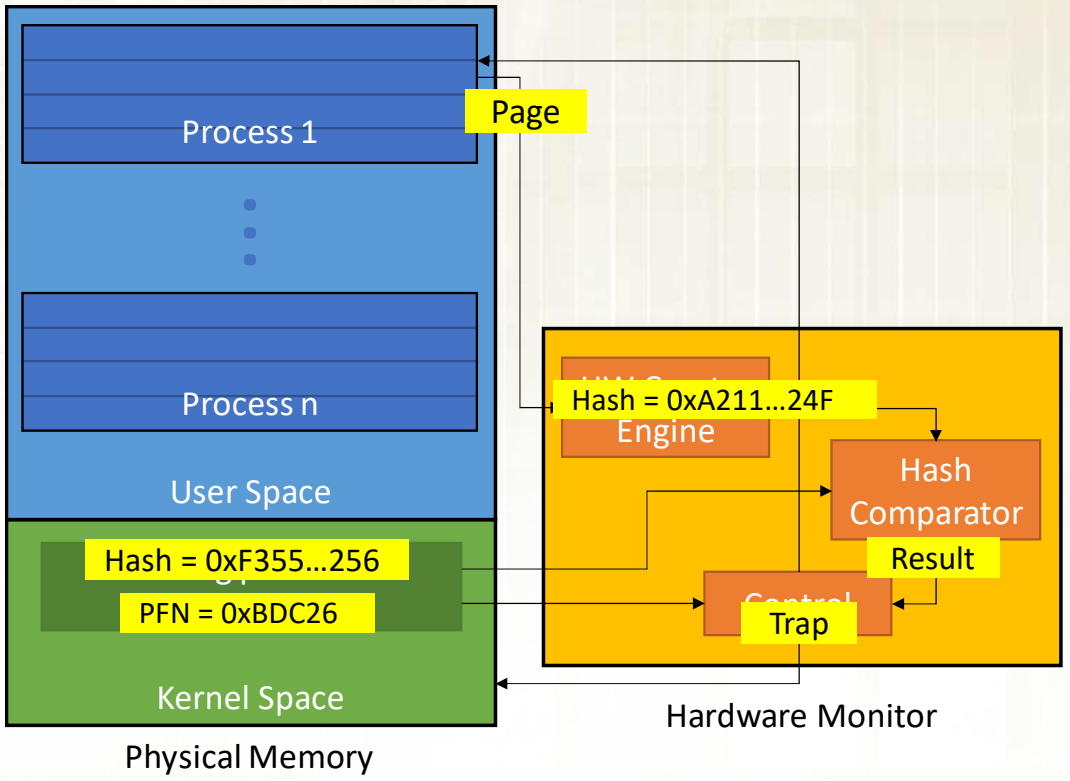


A True Story about Publishing

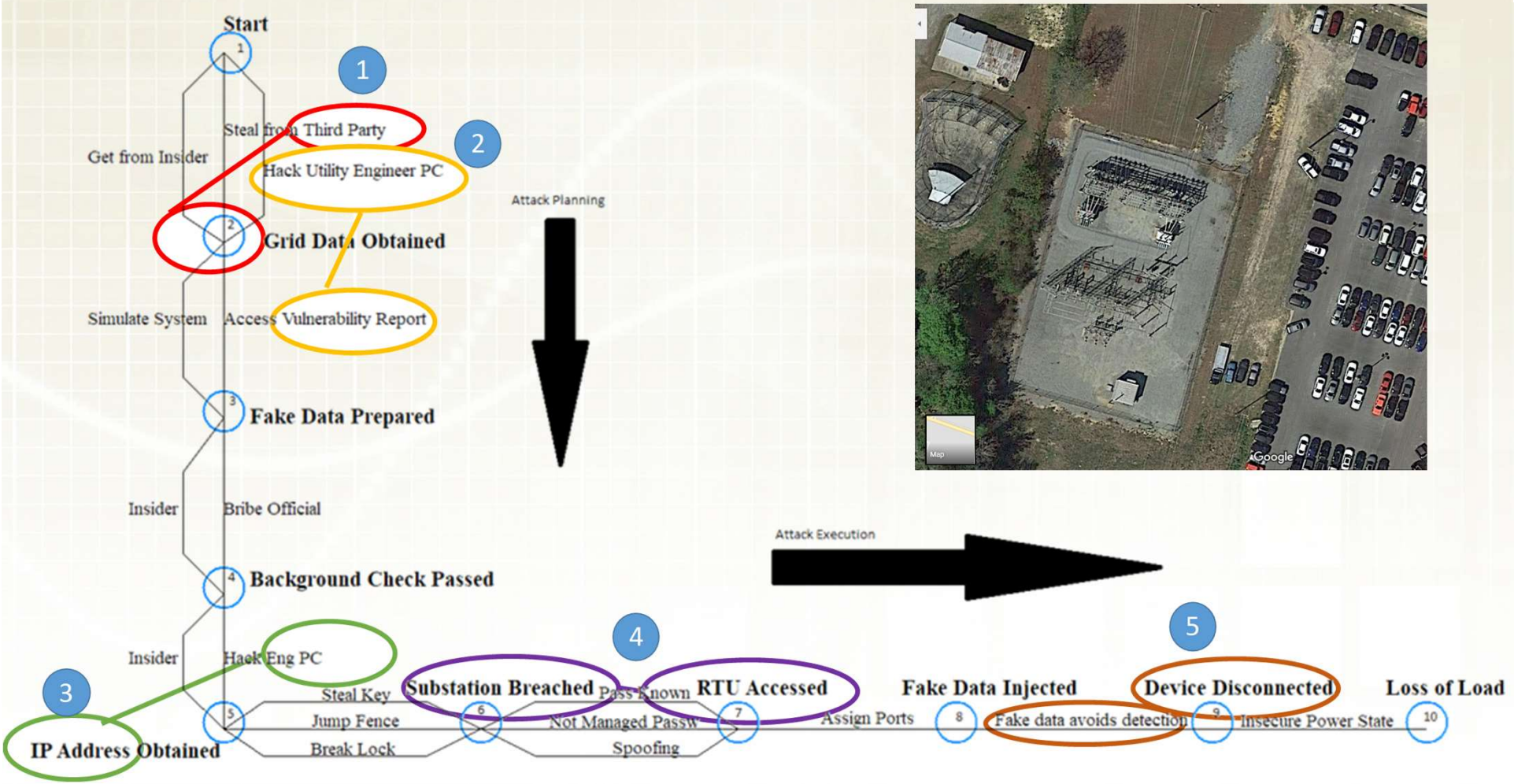
- During my Ph.D., Nanni was General Chair of DAC
  - Nanni said that he would not put his name on any paper submission even though it was allowed
  - He said I could submit a paper, but I waited
- I have been General Chair or Program Chair many times in my career
  - I have followed Nanni's example every time

Memory Hash

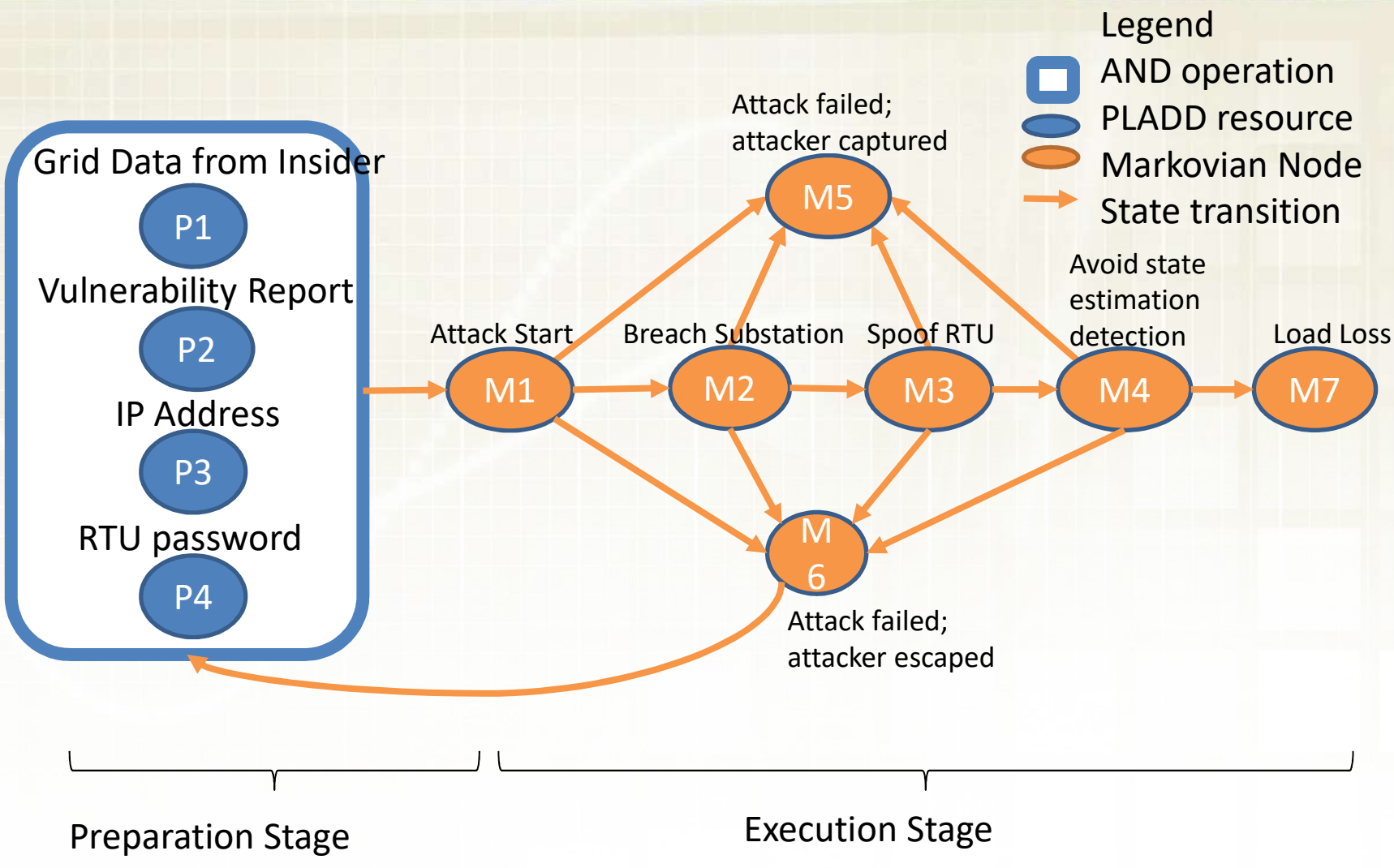
- Page-based memory monitoring of a fetched physical address
- Kernel fetches golden hash of the page pointed to by the PFN
- PFN is passed to the hardware monitor along with the page's hash (signature)
- Hardware monitor
  - Fetches page from memory over AXI bus
  - Generates hash in hardware
  - Compares generated hash to the one passed from Kernel



Power Grid Attack Scenario



Game Theoretic Model and Analysis



Random Encodings and Computation

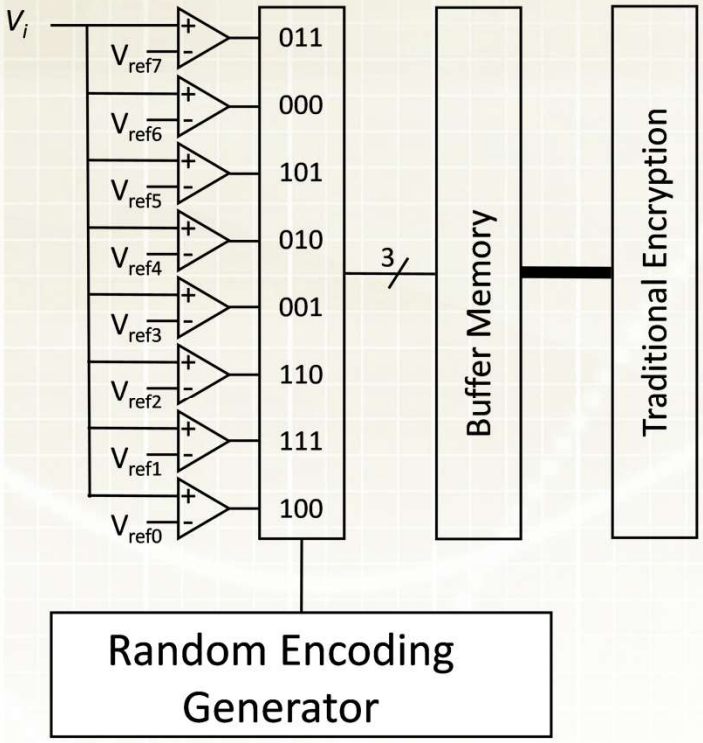


Figure 4: Random Sensing with RanCode

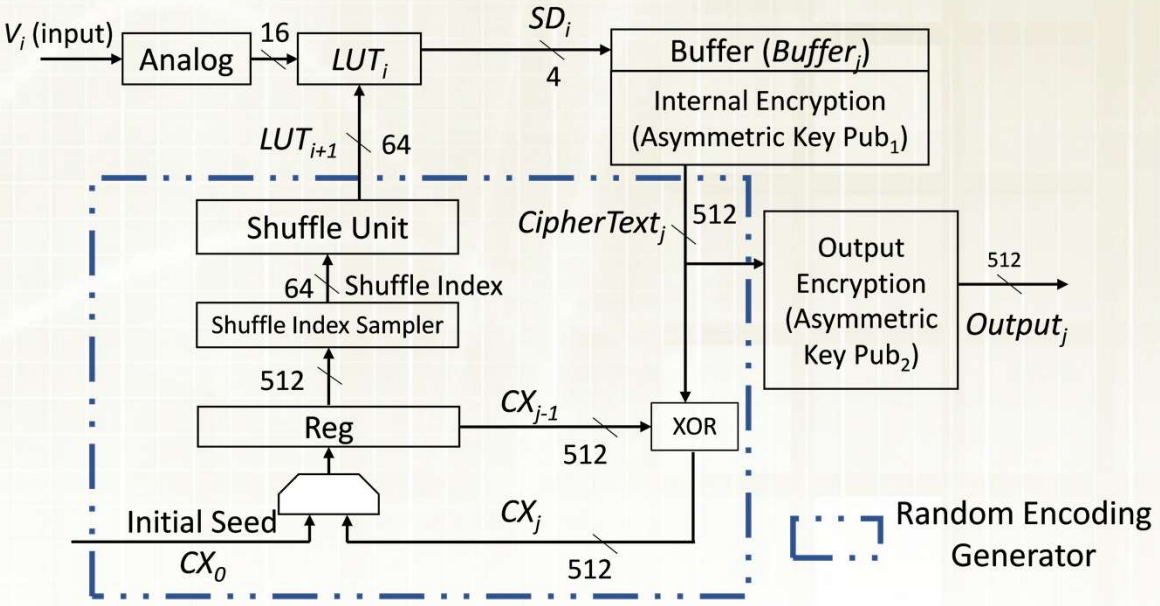
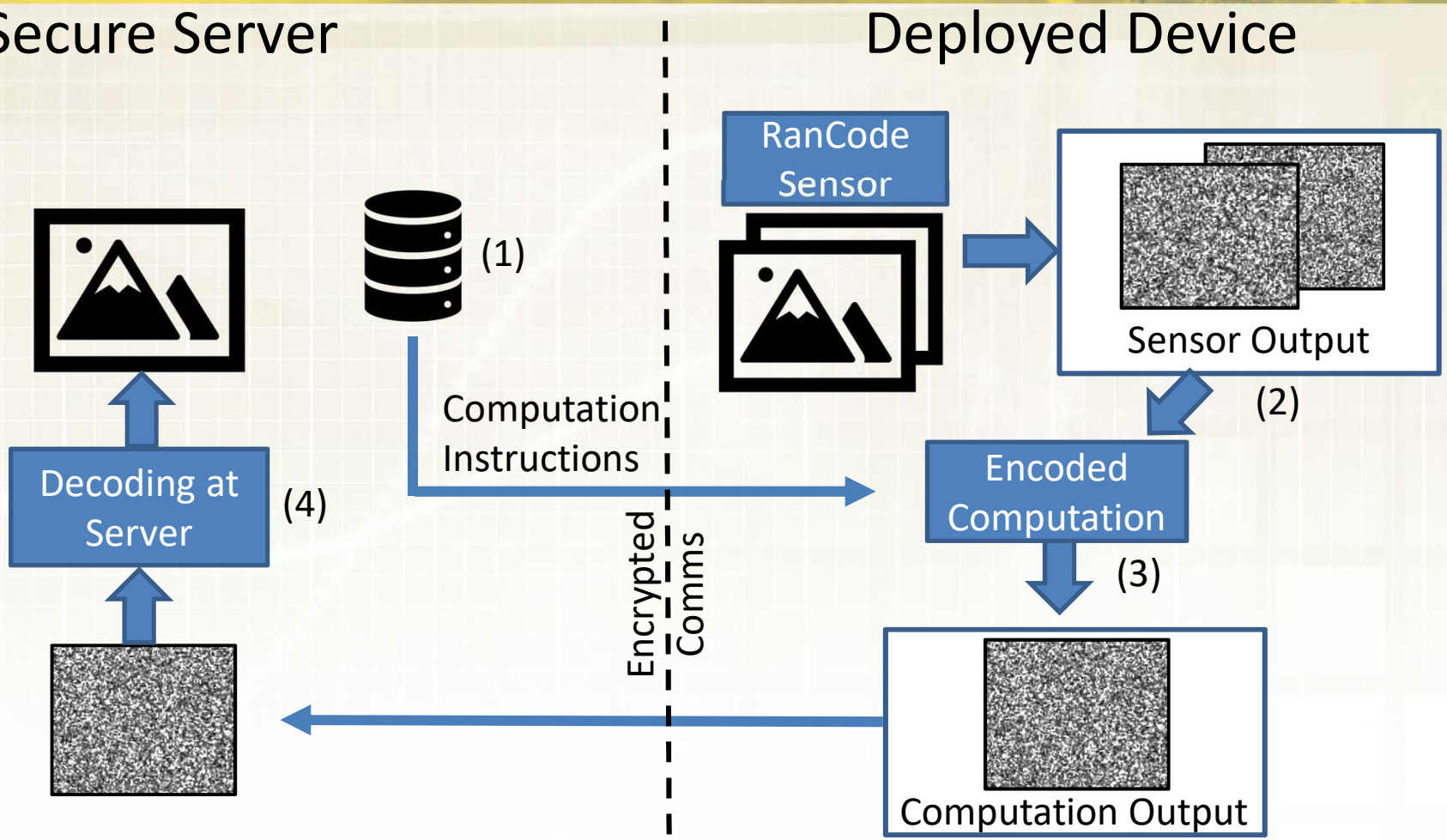


Figure 5: Full Diagram of Rancode Architecture

RanCompute Privacy Homomorphism



K. Hutto and V. Mooney, "Implementing a Privacy Homomorphism with Random Encoding and Computation Controlled by a Remote Secure Server," *ACM Transactions of Embedded Computing*, 2024.

A Final True Story

- In 1998 I interviewed at GT, UTAustin, Cornell, Johns Hopkins and four more…
- I showed Nanni my draft slides
- The last slide said “Future Research Ideas” and was empty
  - Nanni asked if I wanted his advice on this slide
  - I said no
  - Nanni said OK
- Message: respect for students