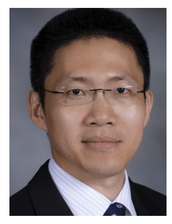
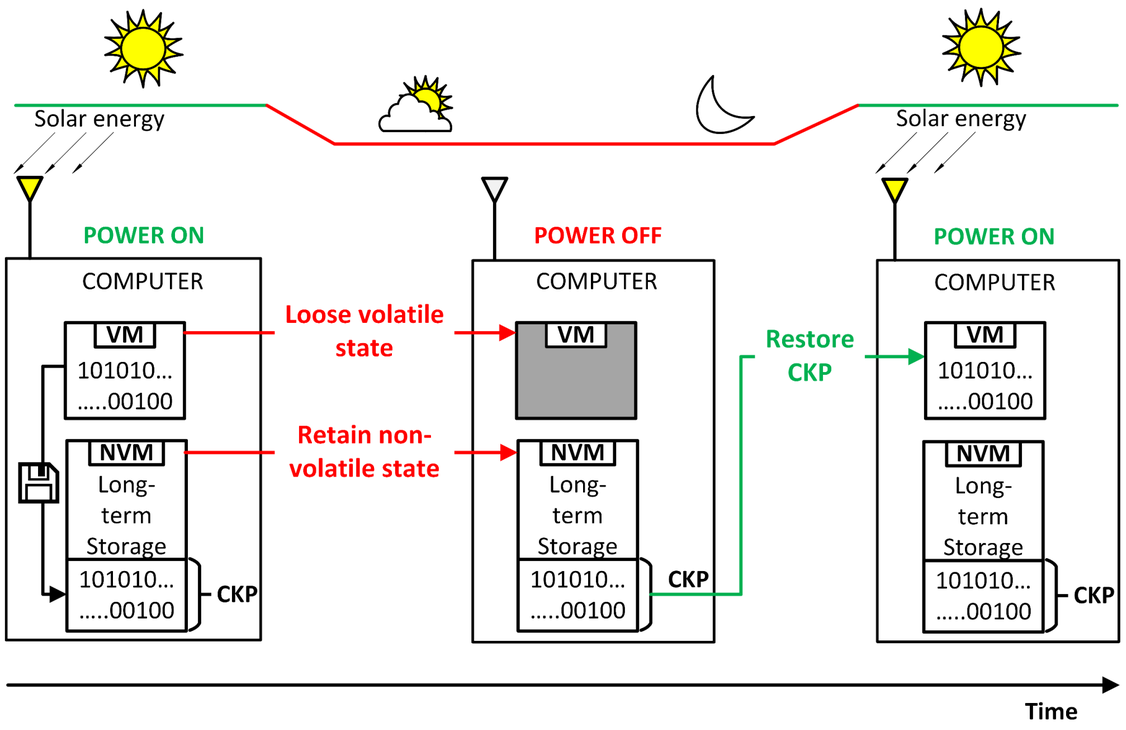
SaTC: CORE: Medium: Collaborative: Energy-Harvested Security for the Internet of Things



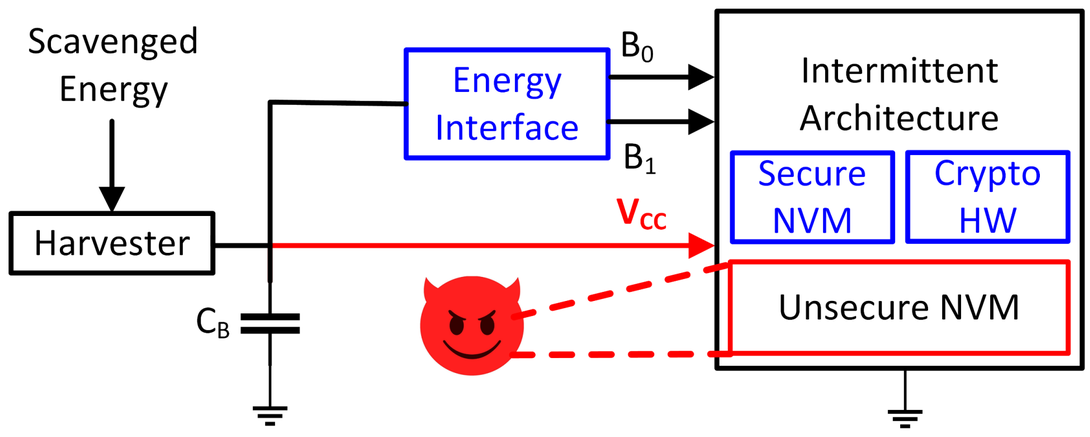


Patrick Schaumont (Virginia Tech), Dong Ha (Virginia Tech), Chao Wang (USC)

1. Intermittent Computing

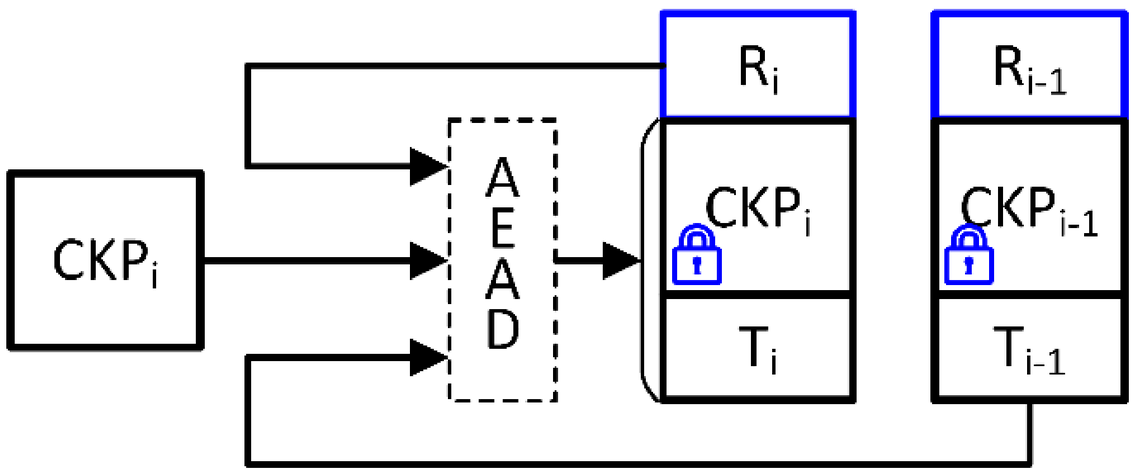


2. Attacker model



- **Energy interface:** Indicate the level of energy in C_B
- **Secure NVM:** Root of trust, store a section of CKP
- **Crypto HW:** Fast and energy efficient cryptography

3. Secure Intermittent Computing



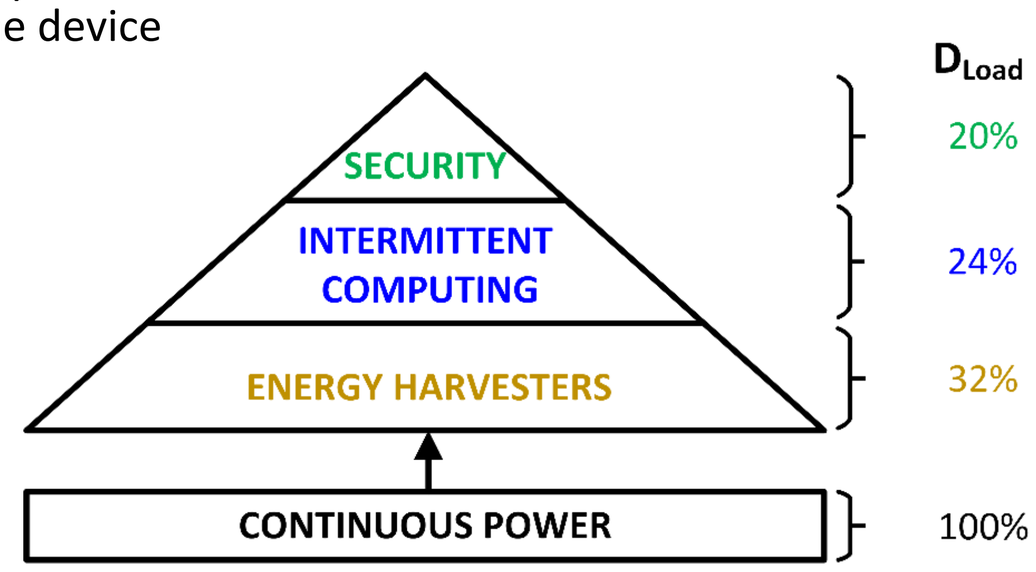
- **Freshness**
- **Information Security**
- **Atomicity**
- **Continuity**

4. Implementation

$$D_{Load} = \frac{P_{Input}}{P_{Load}}$$

Application: ECDH
Checkpoint size: 1211B

- D_{Load}: Duty cycle of the device running ECDH
- P_{Input}: Power supplied to the device
- P_{Input} = 2mW
- P_{Load}: Power required by the application



5. Broader Impacts

- **Courses**
  - ECE 5284 Power Management Circuits for Energy Harvesting
  - ECE 5520 Secure Hardware Design
  - ECE 5580 Cryptographic Engineering
  - CSCI 599 Automated Reasoning and Verification (at USC)
- **Internship**
  - Archanaa Krishnan (Texas Instruments, Summer 2019)
  - Jiayu Li (Texas Instruments, Summer 2019)

References

- C. Suslowicz, A. Krishnan, P. Schaumont, "Optimizing Cryptography in Energy Harvesting Applications," 2017 Workshop on Attacks and Solutions in Hardware Security (ASHES), Dallas, TX, November 2017.
- C. Suslowicz, A. Krishnan, D. Dinu, P. Schaumont, "Secure Application Continuity in Intermittent Systems," 9th International Green and Sustainable Computing Conference (IGSC18), Pittsburgh, PA, 2018.
- A. Krishnan, P. Schaumont, "Exploiting Security Vulnerabilities in Intermittent Computing," 8th International Conference on Security, Privacy and Applied Cryptography Engineering (SPACE 2018), Kanpur, India, 2018.
- A. Krishnan, C. Suslowicz, D. Dinu, P. Schaumont, "Secure Intermittent Computing Protocol: Protecting State Across Power Loss," Design Automation and Test in Europe (DATE 2019), Florence, IT, March 2019.
- D. Dinu, A. Krishnan, P. Schaumont, "SIA: Secure Intermittent Architecture for Off-the-Shelf Resource-Constrained Microcontrollers," IEEE International Symposium on Hardware Oriented Security and Trust (HOST), May 2019.
- A. Krishnan, P. Schaumont, "Hardware Support for Secure Intermittent Architectures (Extended Abstract)," Workshop on Energy-Secure System Architectures (ESSA), May 2019.
- Q. Brogan and D.S. Ha, ."A Single Stage Boost Converter for Body Heat Energy Harvesting with Maximum Power Point Tracking and Output Voltage Regulation. International Symposium on Circuits and Systems (ISCAS), May 2019.
- J. Li, and J.H. Hyun, and D.S. Ha, "A Multi-Source Energy Harvesting System to Power Microcontrollers for Cryptography," 44th Annual Conference of the IEEE Industrial Electronics Society (IECON), Oct. 2018.