ProperData Frontier 2nd Annual Symposium

Privacy-from-Birth: Protecting Sensed Data from Malicious Sensors with VERSA

Ivan De Oliveira Nunes[1], Seoyeon Hwang[2], Sashidhar Jakkamsetti[2] and Gene Tsudik[2]
[1]Rochester Institute of Technology and [2]University of California, Irvine

(Appeared in S&P'22)

Low-end IoT Devices

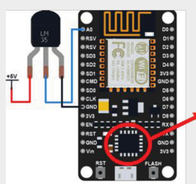

- Low cost, low power, and small size
- Single core, 8/16-bit CPU, <48 MHz and < 64 KB (RAM + FLASH)
- No OS, MMU, MPU, TEE,
- Bare metal (e.g., TI MSP430)

Problem Statement

- Sensors often collect sensitive information
- Resource constrained; lack security features
- Attractive targets for attacks (e.g. Mirai)

Existing Techniques

Just encrypting sensed data does not help

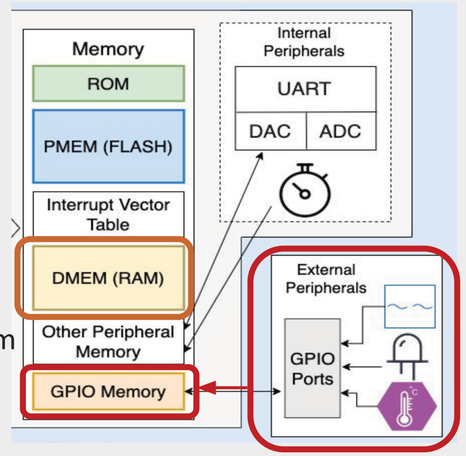


Compromised software (malware) can still extract sensed data!

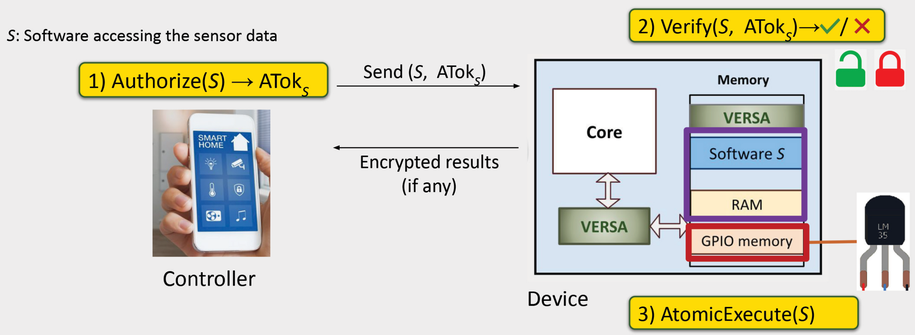
Integrity-ensuring techniques (e.g. remote attestation) can ***detect***, but ***cannot prevent*** leakage

Privacy-from-Birth

- "All traces of sensed data must be protected from *birth* until it *leaves the device*"
  whenever data becomes digital
- PfB Goals:
  - Prevent access to GPIO memory except for authorized software
  - Provide a secure execution platform for authorized software to process sensed data



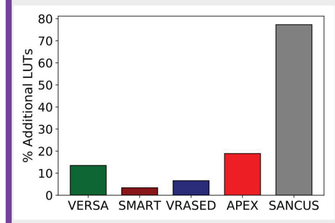
VERSA: Verified Remote Sensing Authorization Architecture



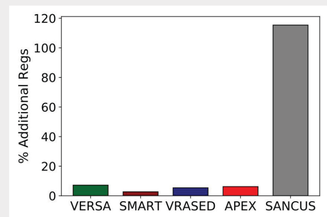
- Access Control to Sensed Data
- Atomic Execution of the Authorized Software *S*
- Data Erasure at Reboot/Reset

Implementation/ Evaluation

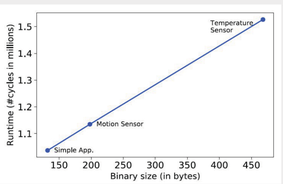
- VERSA is implemented on OpenMSP430
- Synthesized and deployed on Basys3 FPGA
- 13% hardware overhead over OpenMSP430
- 10% hardware overhead over VRASED
- O(n) runtime for request verification



#Look-Up Tables



#Registers



Takeaways

- PfB guarantees end-to-end privacy assurance for sensor data in low-end MCUs
- VERSA provably realizes PfB with a minimal formally verified hardware (open-sourced)
- 13% hardware overhead and linear runtime for verification

SaTC Frontiers: Collaborative: *1956393* [1], *1955227* [2], *2103439* [3], *1956435* [4]
Institutions: UC Irvine [1], Northeastern Univ. [2], UC Davis [3], USC [4]
Lead PIs: A. Markopoulou [1], D. Choffnes [2], Z. Shafiq [3], K. Psounis [4]