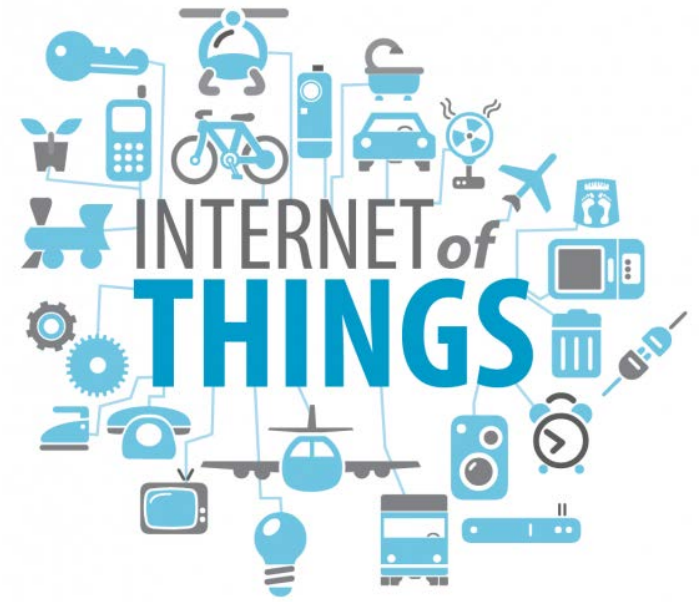
하드웨어 기능을 활용한 임베디드 시스템 보안 연구

부산대학교 정보컴퓨터공학부
권동현 교수

부산대학교
PUSAN NATIONAL UNIVERSITY

Embedded System Security

- 사물인터넷 시대 도래
- 임베디드 시스템의 보안 중요성 증대
  - 스마트 TV 등 스마트 가전에 탑재된 카메라 해킹
  - 임베디드 기기가 탑재된 의료기기의 오동작 유도
  - 스마트 카에 탑재된 센서 정보 변조

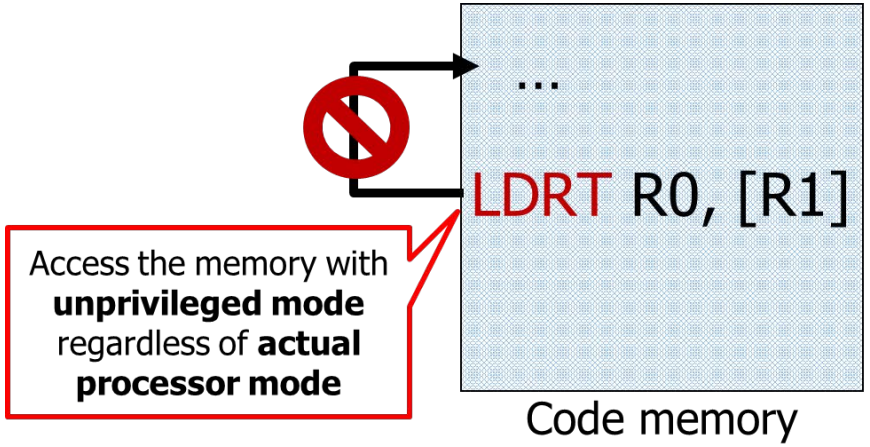


But, in low-end embedded systems..

- Constrained computing resources
  - Low cost, low power consumption
  - Small memory, Low CPU clock speeds
- Lack of processor architectural supports
  - No MMU (no virtualization)
  - Few security extensions

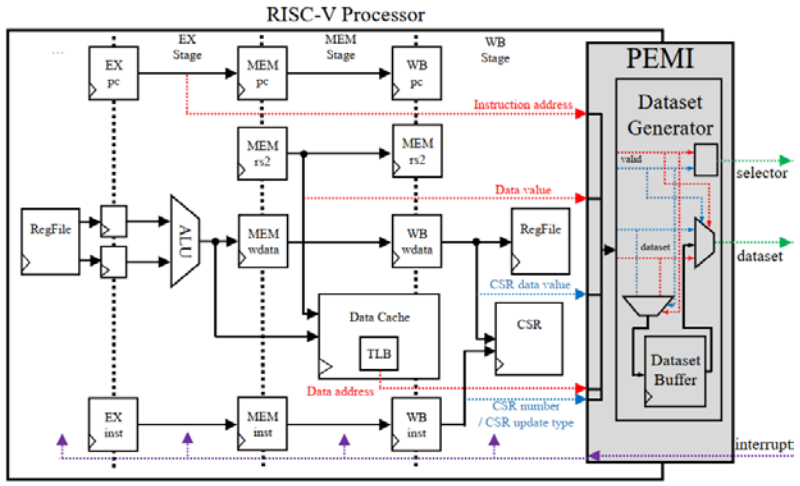
1. Use Existing Hardware Features

- uXOM: Efficient eXecute-Only Memory on ARM Cortex-M
  - Presented at USENIX Security '19
  - eXecute-Only-Memory (XOM)
    - Use as a primitive for many security solutions
    - Already provided in high-end processor architecture
  - uXOM
    - Use unprivileged memory instructions (LDRT, STRT) in ARMv7-M
- Other features
  - ARM TrustZone-M



2. Add New Hardware Features

- RiskiM: Toward Complete Kernel Protection with Hardware Support
  - Presented at Design Automation and Test in Europe (DATE) '19
  - Integrity Monitor
    - Monitor various system behaviors
    - Memory events, system configuration, executed instructions …
  - Add special hardware interface for this
- Next step
  - Add special instructions for security



Conclusion

- Embedded system security
  - Using existing hardware features
  - Adding new hardware features
- There are opportunities
  - Numerous use cases
  - RISC-V open source ISA

- Contacts
  - E-mail: kwondh at pusan dot ac dot kr
  - Site: https://sites.google.com/view/csl-pnu