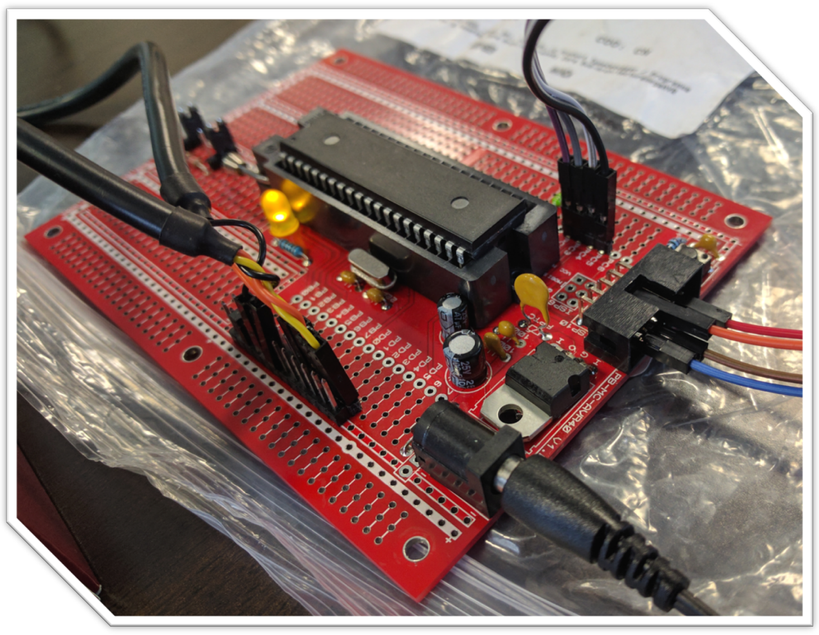
RSAC Security Scholar

Firmware Security on Commodity Hardware 2017 MITRE Embedded CTF

Tiemoko Ballo
Carnegie Mellon University, Information Networking Institute

Problem Statement and Goals



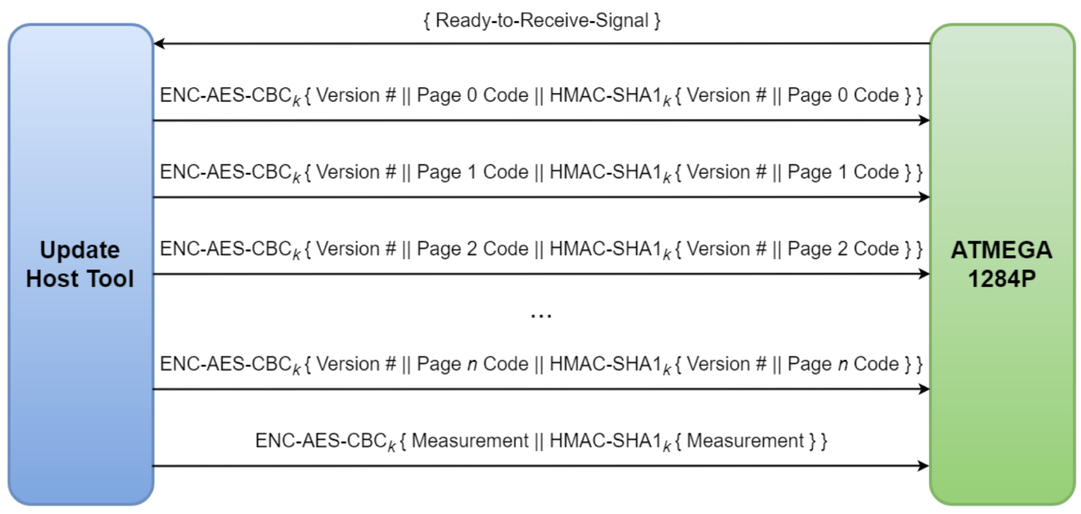
ATMEGA 1284P
(128K Flash, 4KB EEPROM, 16KB SRAM)

- Goal - design and implement a bootloader for secure firmware distribution as part of the 2017 MITRE Embedded CTF, the only attack-and-defense CTF that both uses real hardware and requires teams to build targets (invite-only, 10 universities).
- Functional Requirements - on a resource-constrained microcontroller (ATMEGA 1284P) without dedicated security hardware, the system must:
  - Support firmware update
  - Allow memory readback for an authenticated technician
  - Disallow firmware version downgrade
- Security Requirements – despite an adversary with physical access and full source code, the design must ensure:
  - Secrets can't be read from device memory or a firmware image (confidentiality)
  - Bootloader only accepts factory-issued firmware (authentication)
  - Only unmodified firmware images are loaded (integrity)

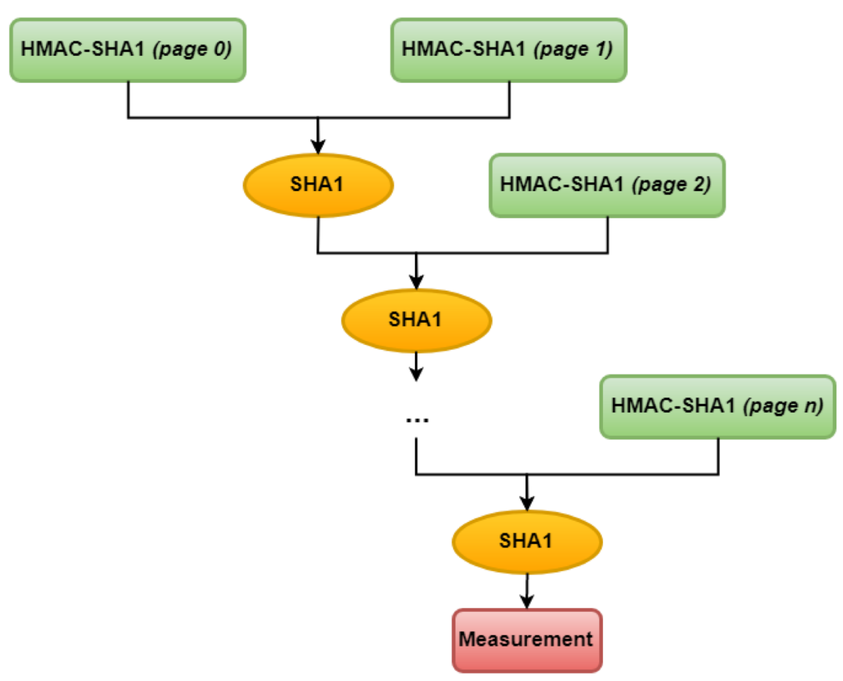
Approach

- Well-vetted Cryptographic Algorithms:
  - AES-256-CBC to protect firmware pages
  - HMAC-SHA1 for integrity and data-origin authentication
- On-boot Verification:
  - SHA1/HMAC-SHA1 chained measurement across firmware pages
  - Integrity check of 30KB firmware with only 16KB of SRAM
  - Measurement stored in lock-bit protected memory
  - Measurement verified on boot, firmware erased if check fails
- ELF Section Relocation to Alleviate Memory Constraints:
  - Portability: static libraries moved to lower 64KB of flash, permitting AVR standard 16-bit pointers without re-write
  - Flexibility: some privileged functions moved to app memory, key material passed on SRAM stack and erased after use
- Introducing Noise for Side-channel Resilience:
  - Spurious per-round en/decrypt operations on inverse data
  - Power trace noise thwarts default AES timing profiles
- Unpredictable Checks for Fault Injection Resilience:
  - Multiple complementary checks for all critical branches
  - Pseudo-random delay (inlined spin-wait) between checks

Update Protocol



Firmware Measurement



Results

- Design won "Iron Flag" award for withstanding all attacks (software exploitation, side-channel key extraction, and fault injection) for the entirety of the competition's 6 week attack phase – despite attackers with full source code and physical access.
- Placed 3rd overall, 19 attack flags collected across 5 teams and all 6 categories.
- Lessons for Future Designs:
  - ECC combines benefits of asymmetric scheme (no signing private key on device) with key size comparable to symmetric scheme
  - Switch from on-board oscillator to microcontroller's internal clock during sensitive operations for robust clock glitching defense
  - For general purpose devices, ensure that any code relocation does not overlap with interrupt vector table
- Acknowledgements:
  - Competition Advisor: Professor Martin Charlisle
  - Competition Team Members: Surbhi Shah, Mark Horvath, Saurabh Sharma, Karthic Palaniappan, Pouria Pezeshkian