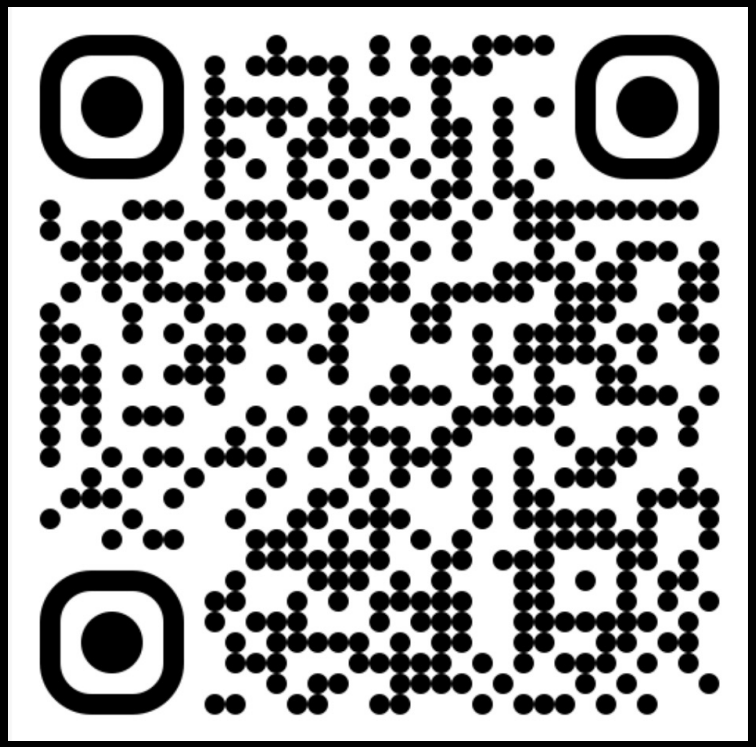
Software Security Issues for Small IoT SoCs

Stephen Cravey - Decemeber 14, 2024

From my MSc Dissertation
Graduation at RHUL on Thursday

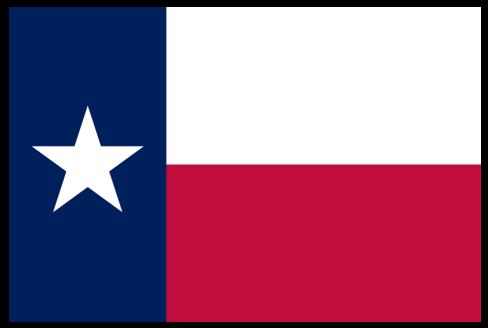
SETEC Astronomy

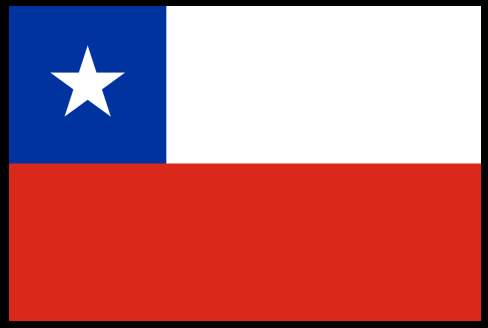


Agenda

- Introduction
- Foundations
- SoCs
- Binding
- PUFs
- Governance
- Lessons Learned
- Questionnaire
- Questions

Introduction





About

- Apple II
- Software
- Electronics
- 2600
- Unix
- ECE/VLSI
- ISP Architect
- BGP Monkey
- DFIR
- Military/Defense
- NASA ISS Program
- Recovering CISO
- Big Consulting
- cravey@gmail.com

Foundations - Internet

- Network of Networks

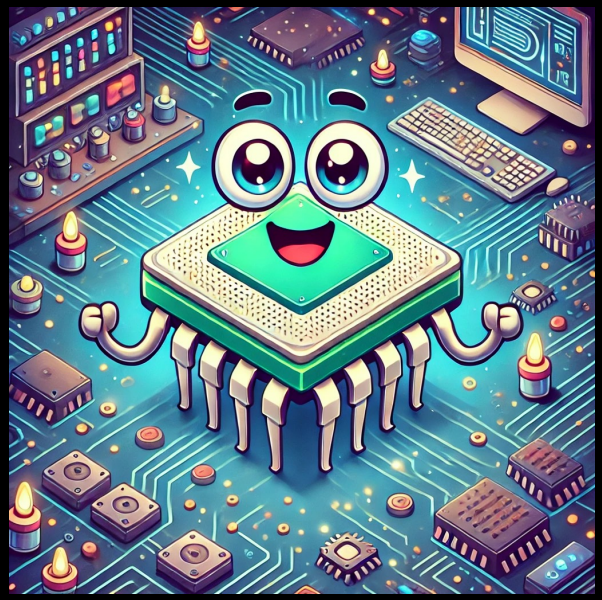
Foundations - IoT

- Coined ~2005 by ITU
- Things are EVERYWHERE!

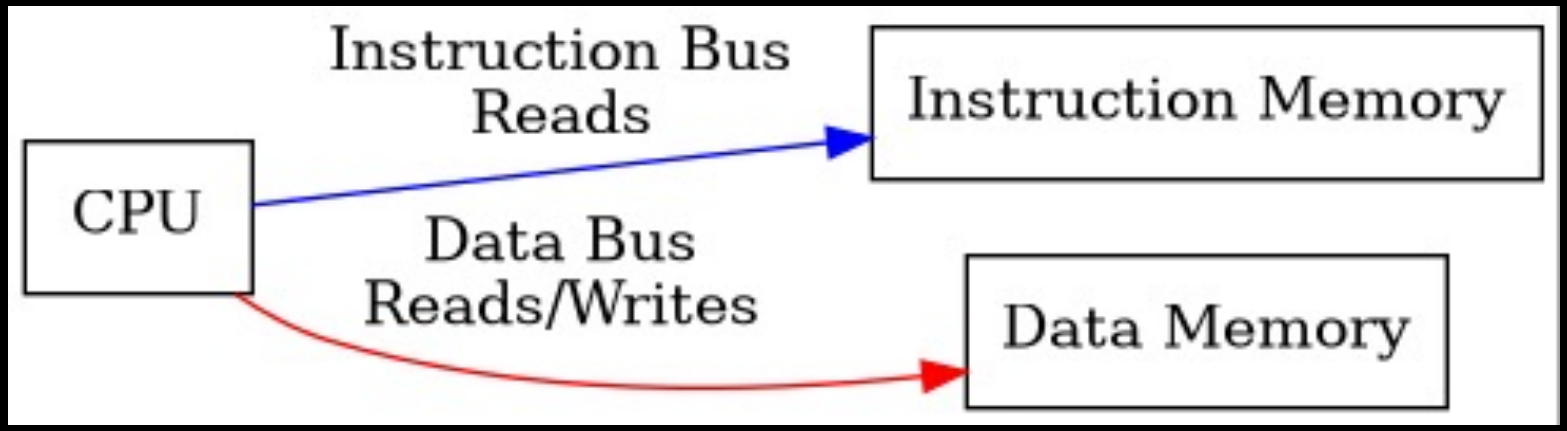
Foundations - Microprocessors

- Takes INPUT
- Performs some operation (Processes INPUT)
- Provides OUTPUT

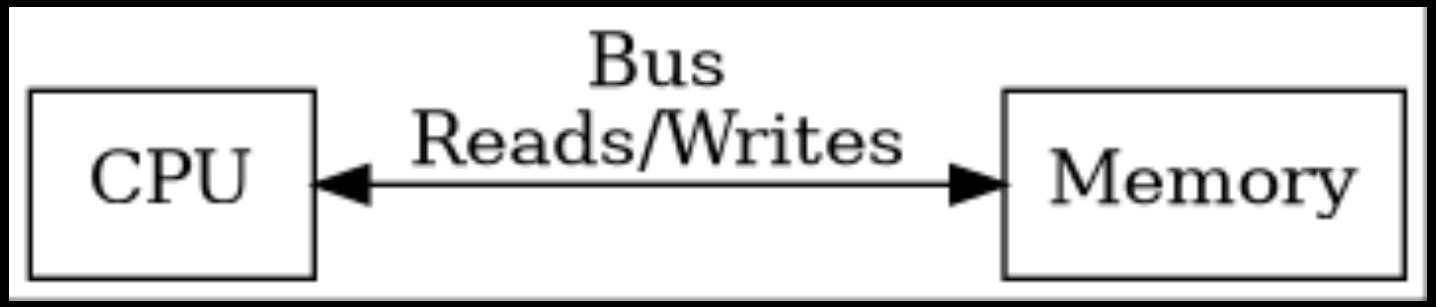
- https://itema-as.github.io/6502js/



Foundations - Microprocessors
Harvard Architecture

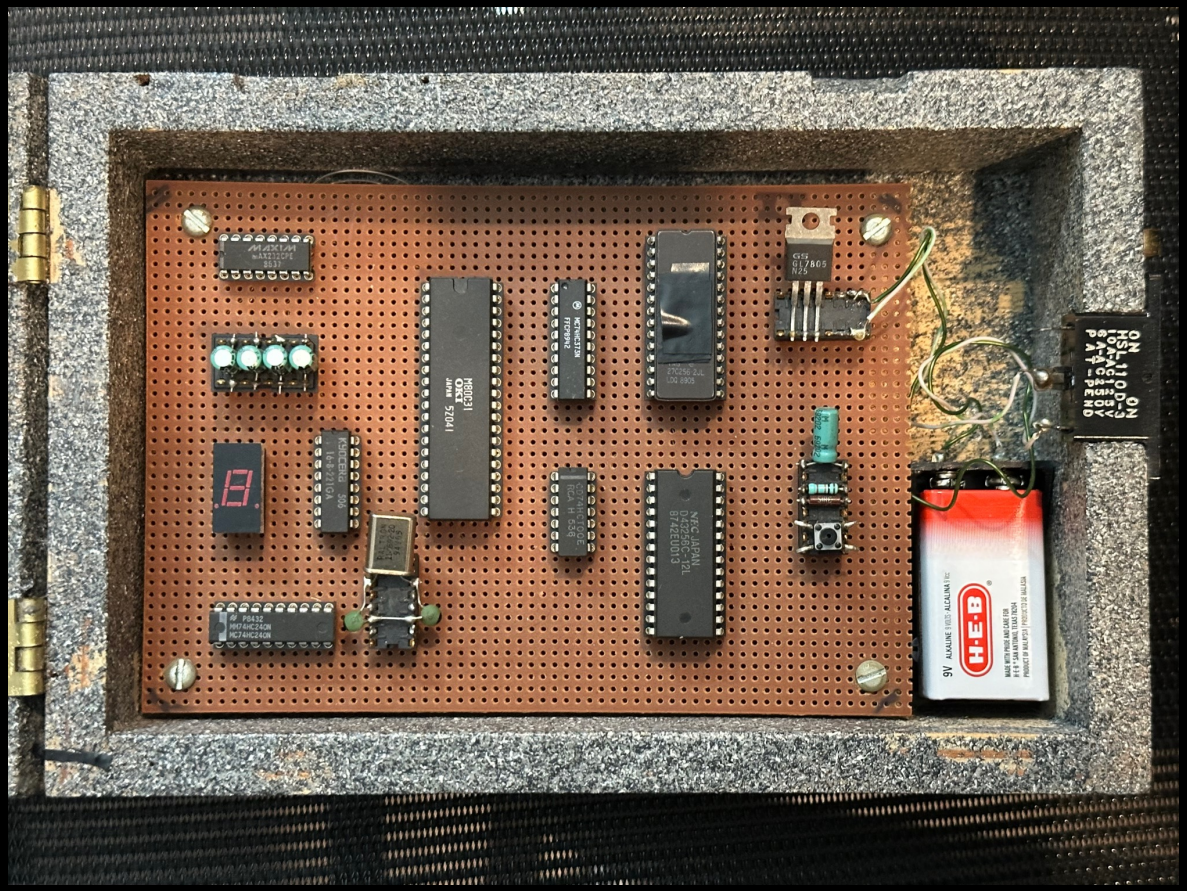


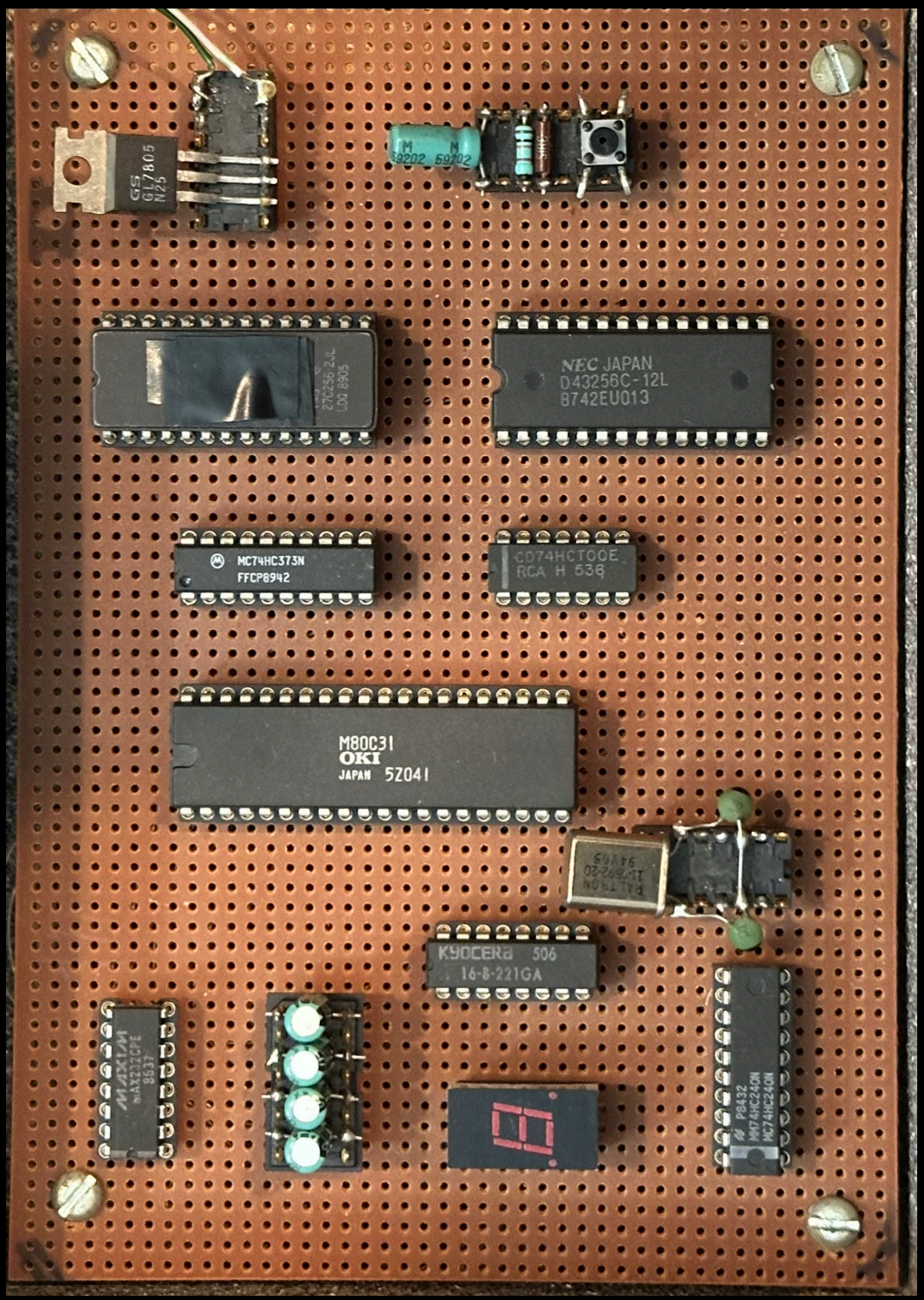
Foundations - Microprocessors
von Neumann Architecture



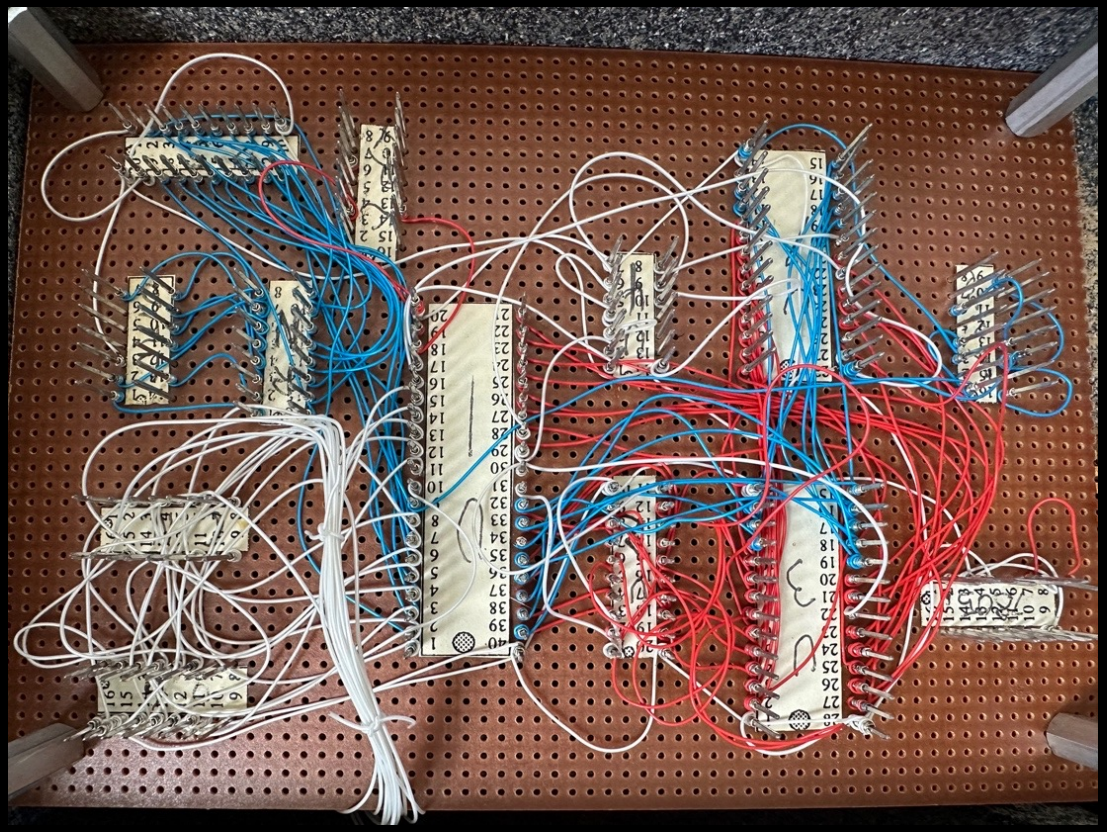
Foundations - SoCs

Foundations - SoCs



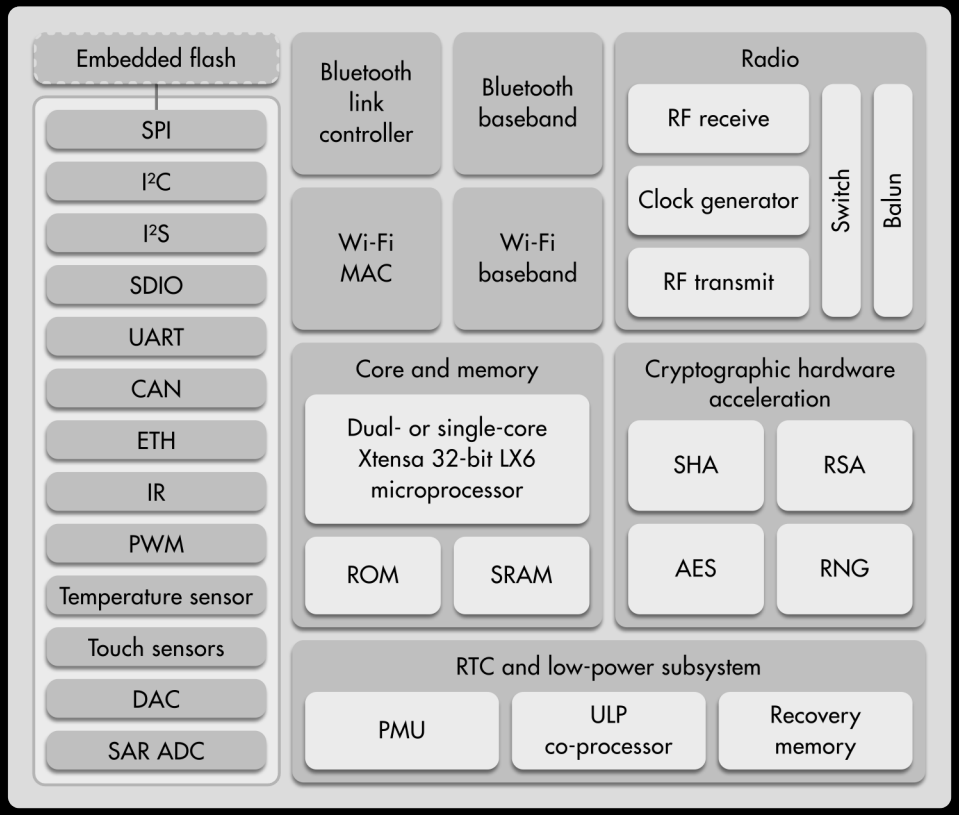

GS
GL7805
N25
NEC JAPAN
D43256C-12L
8742EU013
MC74HC373N
FFCP8942
CD74HCT00E
RCA H 536
M80C31
OKI
JAPAN 5Z041
KYOCERA 506
16-8-221GA
MAXIM
MAX232CPE
8537
P8432
MM74HC240N
MC74HC240N

Foundations - SoCs



Foundations - SoC Drawer

Foundations – SoC Block Diagram



Foundations - Binding Software to Hardware

- Software can only run on approved hardware
- Copy Protection, etc.

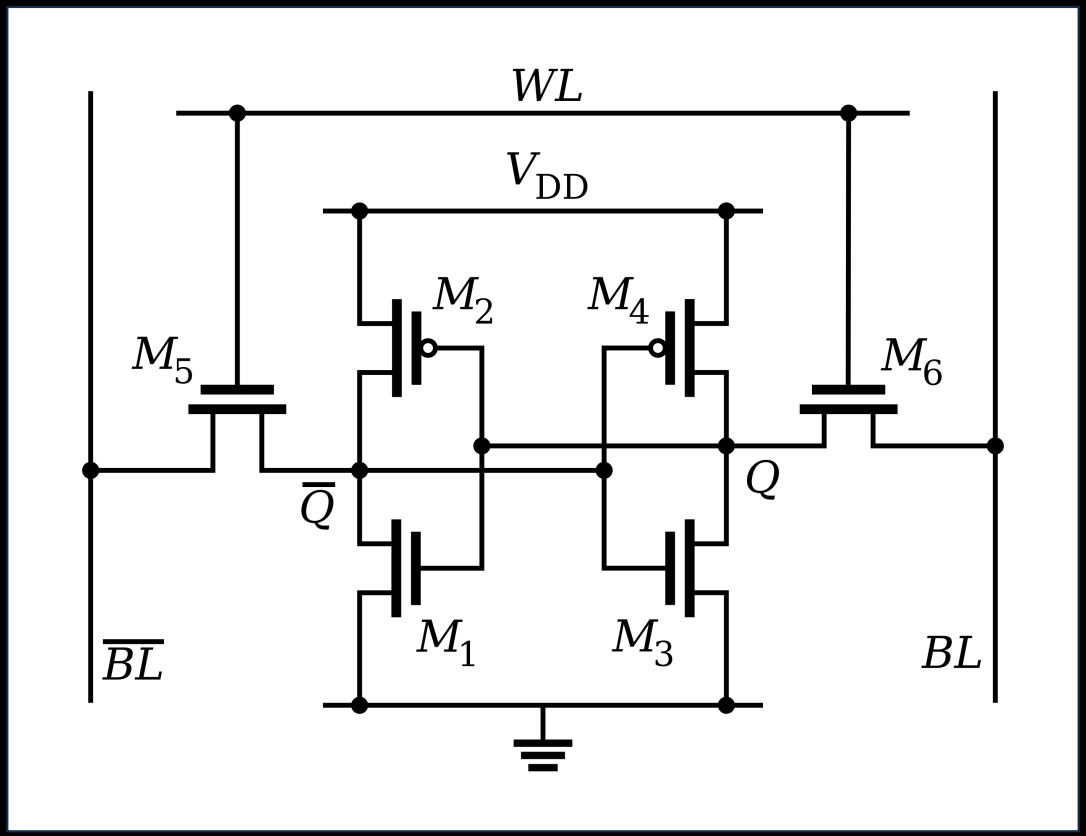
Foundations - Binding Hardware to Software

- Prevents Hardware from executing unapproved software

Foundations - PUFs

- Physically Unclonable Functions?
- Physically Unclonable Features?
- Physical Unclonable Features?
- Referred to as a “*-PUF”

Foundations - SRAM PUF



Foundations - HSM

- Hardware Security Modules
  - Provide basic cryptographic capabilities.
    - Unique Identifiers
    - TRNG
    - Misc Other Features

Context – PUF Practicality

- It’s hard to manage databases of PUF fingerprints
- PUF is often subject to environmental changes
- Computationally complex to properly model in a way that allows for environmental changes

SoC Selection Criteria

- Harvard Architecture
- Distinct ISAs
- **No NDA for technical data**
- Something I’ve encountered in my daily life

SoCs Selected

- EspressIF 8266
- Espressif ESP32
- Microchip PIC32
- Microchip AVR-BLE ATMega3208
- Sliicon Labs Gecko BGM111
- Raspberry Pi RP2040

Lessons Learned

- For small, common IoT SoCs, security is often not a priority.
- More expensive SoCs are often better.
- Devtools often kindof suck.
- Quality embedded development is harder than expected.
- Open season on many IoT devices!

Questionnaire

Questionnaire

- What is the CPU Family of the SoC?
- How much program memory is available?
- Is there a way to read protect program memory?
- Are there vulnerabilities in the read protect capability?
- Is there a way to write protect program memory?
- Are there vulnerabilities in the write protect capability?
- Are there Secure Boot capabilities?

Questionnaire

- Are there vulnerabilities in the Secure Boot Capability?
- Is there effective protection against power analysis attacks?
- Is there effective protection against power glitching attacks?
- Is the attack surface for the SoC well understood?
- Is there an SDK required for use of the features needed for the end product?
- What is the process for recompiling against new versions of the SDK?
- What is the process for updating the software on the SoC?

Questionnaire

- Are there components of the SoC with contain software that cannot be field updated, or updated at all? E.g. radio baseband software?
- If there is an SDK or built in software, does the manufacturer have a track record of providing regular updates?
- Does the manufacturer have a track record of vulnerabilities that are difficult to remediate?
- Does the manufacture address security vulnerabilities diligently?
- Does the manufacturer sponsor a bug bounty program?
- What are the cryptographic capabilities of the SoC?
- Do the cryptographic algorithms meet current standards? (AES256, ECC, etc.)

Questionnaire

- What unique identifiers are present in the SoC? (Serial numbers, network address, etc.)
- What PUFs might you want to use? Does it support those?
- Is there good community support for the SoC?
- Does complete documentation for the SoC require an NDA?
- Is there documentation available about secure workflows for tasks like software updates, read/write locking, etc?
- Is there free support for security related questions form the manufacturer?
- Does the development environment/toolchain run on systems your organization can maintain? e.g. Does it require linux, but your organization only supports Windows?

Questionnaire

- Are the development tools updated regularly?
- Do the development tools have a history of security vulnerabilities?
- Do the development tools have a history of bugs which go for years without being fixed?
- Do the development tools have a secure architecture? E.g. do they have to execute with elevated superuser privileges for non-privileged operations?
- Do the development tools install unnecessary components that load at boot time?
- Is it easy to navigate the documentation repository for the SoC?
- Is it easy to navigate the documentation repository for the development tools?

Questionnaire

- Does the manufacturer have a good reputation in the security community?
- In which country is the manufacturer incorporated?
- In what country is the SoC Fabricated?
- Who actually fabricates the SoC? Is it the manufacturer or a contract FAB such as TSMC?
- What is the geopolitical status of those regions? Is there supply chain risk?
- Are any of the locations prone to influence by the host country's intelligence apparatus? Does this present any risk of illicit introduction of vulnerabilities to serve a national interest?
- Are there any other security capabilities that might be needed and are they present?
- Are there vulnerabilities in any of those capabilities?

Stephen Cravey, MSc (Hons), CISSP

- cravey@gmail.com
- github.com/cravey
- Maybe signal
- Maybe bsky
- Xitter a lot less these days.
- Mostly overwhelmed with Spam