SECURE BOOT

Validates the application against public key stored in OTP

Once activated the following is enforced:

- Cannot be disabled
- Applications must be signed
- Applications must be encrypted
- OTP Key section read disabled
  - Keys can be revoked

BOOTROM

Small code block executed first

- Initializes the system
- Handles transition to application/customer code
- Immutable (some exceptions)
  - Manufacturer only “patch” section
  - Focused-ion-beam (FIB)

Security Implemented Here

- Secureboot
- OTP
- Debug/Readback protections

Notable bug examples

- iPhone bugs (limera1n/checkm8)