





OpenloTSummit Europe

MCUboot: Multi-Image

David Brown





MCUboot

- MCU: microcontroller
- Boot: bootloader
- Root of trust
- Validates images before booting or upgrading



MCUboot memory map

SLOT 1

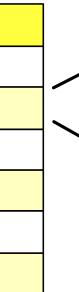
pad

SCRATCH

0x00042000

0x0007c000

0x00080000



Header			
code			
TLV manifest			
pad			
update state			



MCUboot Current Features

- Supports XIP MCUs
- Flash is partitioned into two "slots" and a "scratch area"
- It can validate an RSA or ECDSA signature before booting
- If slot1 is newer than slot0, and valid, it can upgrade
- Upgrade is either overwrite, or swap



XIP (eXecute In Place)

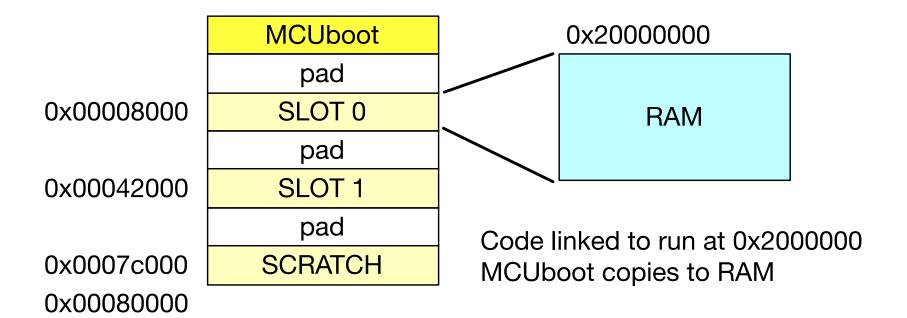
0x0000000	MCUboot		
	pad		
0x00008000	SLOT 0		
	pad		
0x00042000	SLOT 1		
	pad		
0x0007c000	SCRATCH		

0x00080000

code linked at 0x8000 and runs out of flash directly upgrade linked at 0x8000, and must be moved to SLOT 0 to run

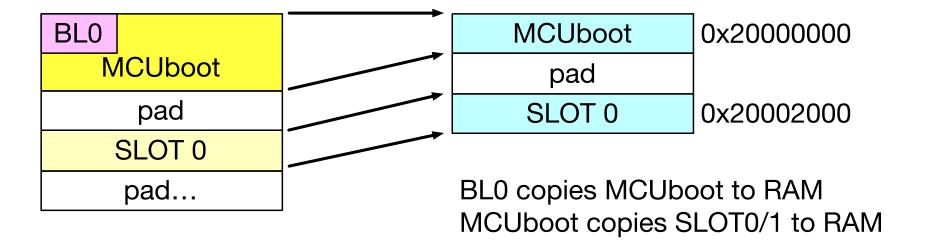


Non-XIP





Non-XIP reality





Multi-image

0x0000000 **MCUboot** pad 0x00008000 SLOT 0 S pad 0x00026000 SLOT 0 NS pad 0x00044000 SLOT 1 S pad 0x00062000 SLOT 1 NS pad 0x0007c000 **SCRATCH** 0x00080000

Header

code

TLV manifest

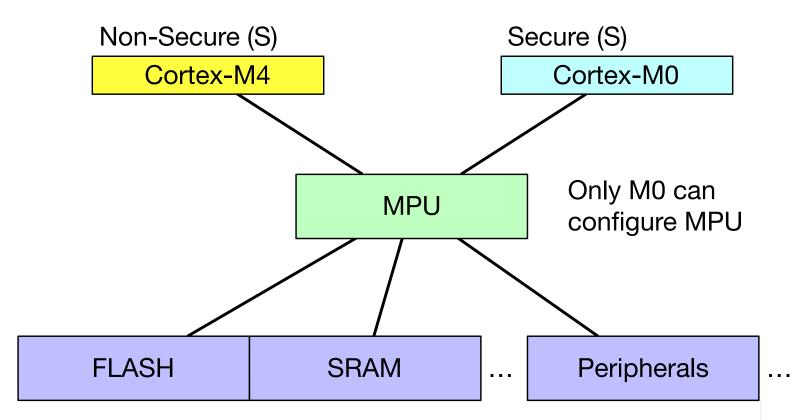
pad

update state

Each slot, same image format

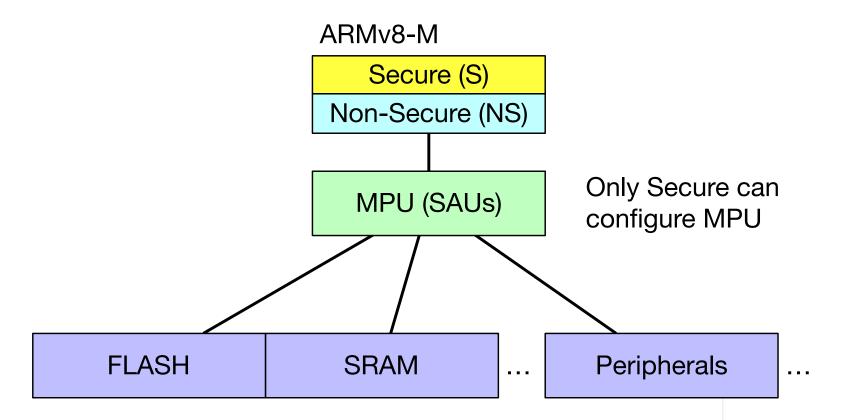


Multiple CPUs



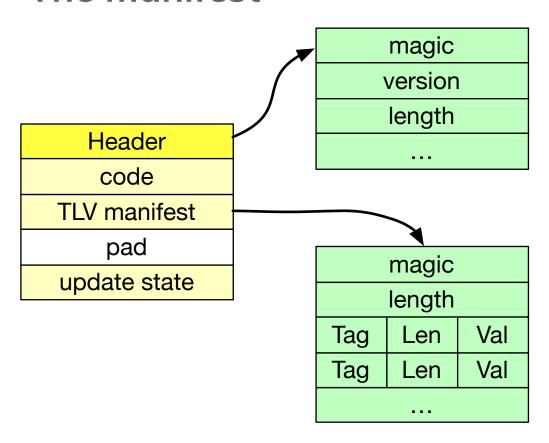


Trusted Execution





The manifest



Example tags

SHA256
Key hash
RSA2048 PSS
Key hash 2
ECDSA256



Multi-manifest

S	lot	0	Secu	re

Header
code
TLV manifest
pad
update state

Slot 1 Secure

Header
code
TLV manifest
pad
update state

Slot 0 Non-Secure

Header
code
TLV manifest
pad
update state

Slot 1 Non-Secure

code				
TLV manifest				
pad				
update state				



Multi-manifest + dependencies

Slot 0 Secure

Header

code

TLV manifest

pad

update state

Slot 0 Non-Secure

Header

code

TLV manifest

pad

update state

Slot 1 Secure

Header

code

TLV manifest

pad

update state

Slot 1 Non-Secure

Header

code

TLV manifest

pad

update state

Tags with dep

SHA256

dep: S < 1.2.6

dep: S > 1.1.0

Key hash

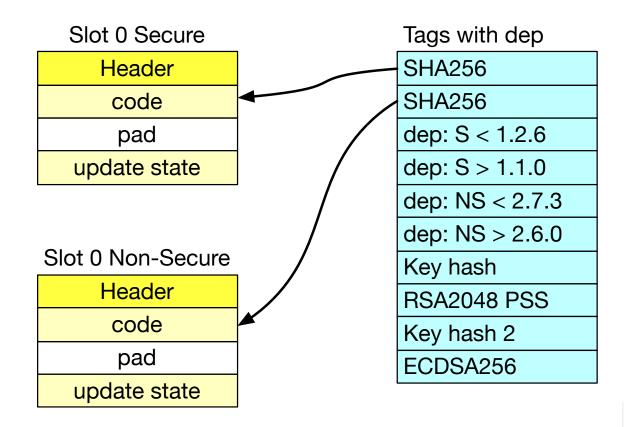
RSA2048 PSS

Key hash 2

ECDSA256



Detached manifest





What is signed?

SHA256

SHA256

dep: S < 1.2.6

dep: S > 1.1.0

dep: NS < 2.7.3

dep: NS > 2.6.0

Key hash

RSA2048 PSS

Key hash 2

ECDSA256

Unprotected

Sig of SLOT 0

Sig of SLOT 1???



Sign the manifest

	S	Н	Α	2	5	6
--	---	---	---	---	---	---

SHA256

dep: S < 1.2.6

dep: S > 1.1.0

dep: NS < 2.7.3

dep: NS > 2.6.0

Key hash

RSA2048 PSS

Key hash 2

ECDSA256

- Sign the first part of manifest
- Protects everything in manifest
- Allows multiple images



SUIT



https://datatracker.ietf.org/wg/suit/about/



COSE SUIT

COSE

protected headers

unprotected headers

payload

signature

SUIT manifest

nonce

sequence (version)

conditions

directives

resources

extensions

all encoded in CBOR

"resources" contains hash of each image



MCUboot plans

- SUIT: wait
- Non-XIP: now
- Multiple images
 - Each with manifest: now
 - o Detached manifest: do we need it?