CLOUDFLARE

Armed to Boot

A Novel Enhancement to Arm's Secure Boot Chain

Derek Chamorro

Ryan Chow

Derek

- Staff Security Engineer

Ryan

- HW Security Engineer

CLOUDFLARE

Overview

CLOUDFLARE

- Cloudflare and Secure Boot Journey
- Hardware Root of Trust
- Background on Arm Secure Boot/Chain of Trust
- Single Domain Secure Boot
- Demo
- BMC
- Future

CLOUDFLARE

What is Cloudflare?

Network Map

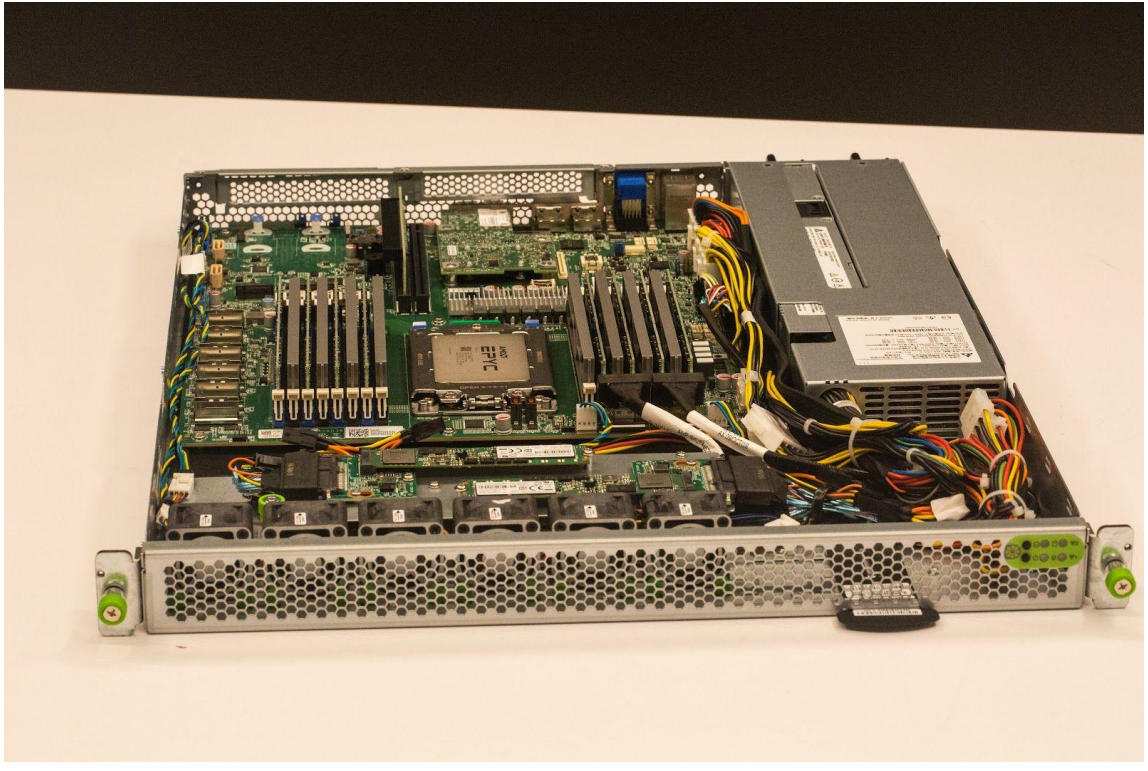
270+
cities in more than 100 countries

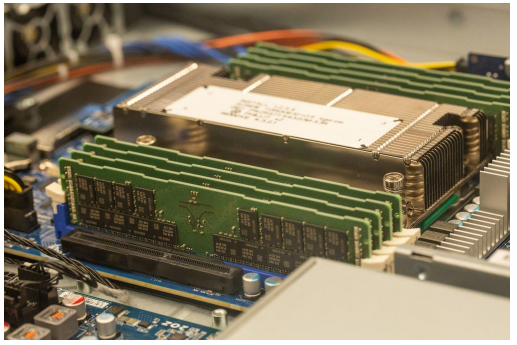
142 Tbps
Of network capacity

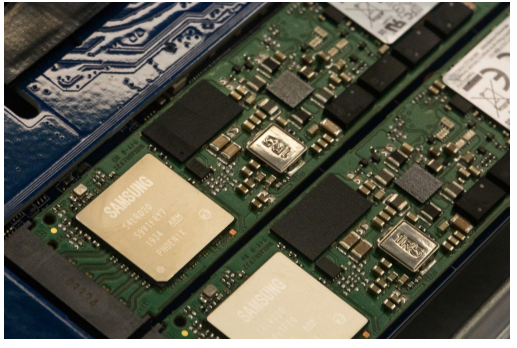
1B+
Unique IP Addresses Daily

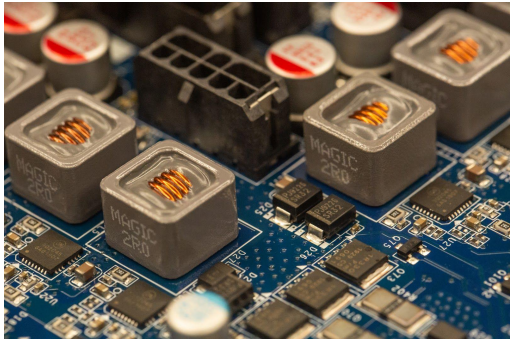
20+MM
Internet Properties

Lots of cities = Lots of servers

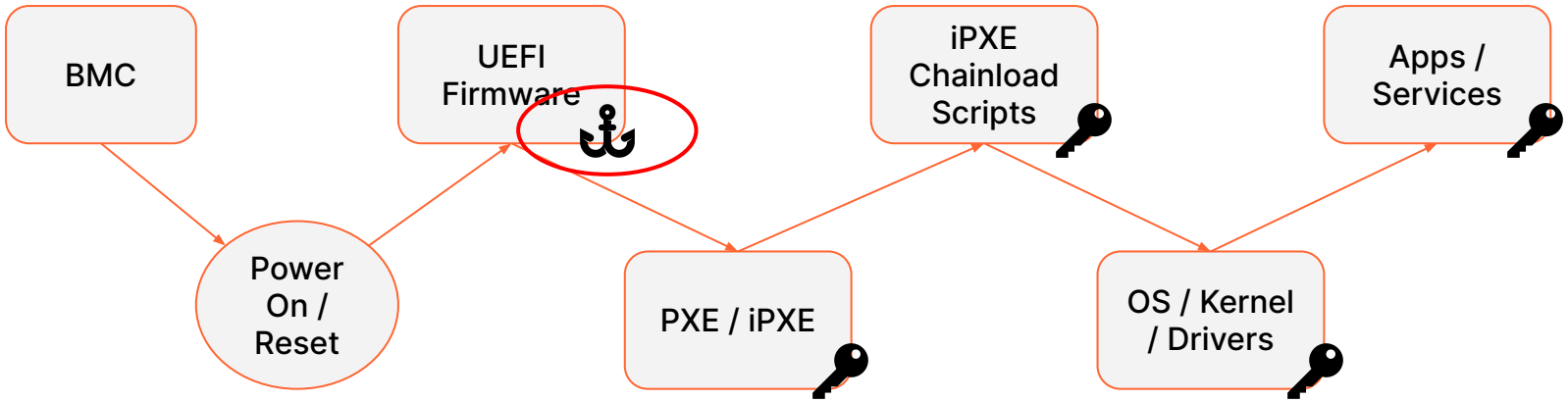


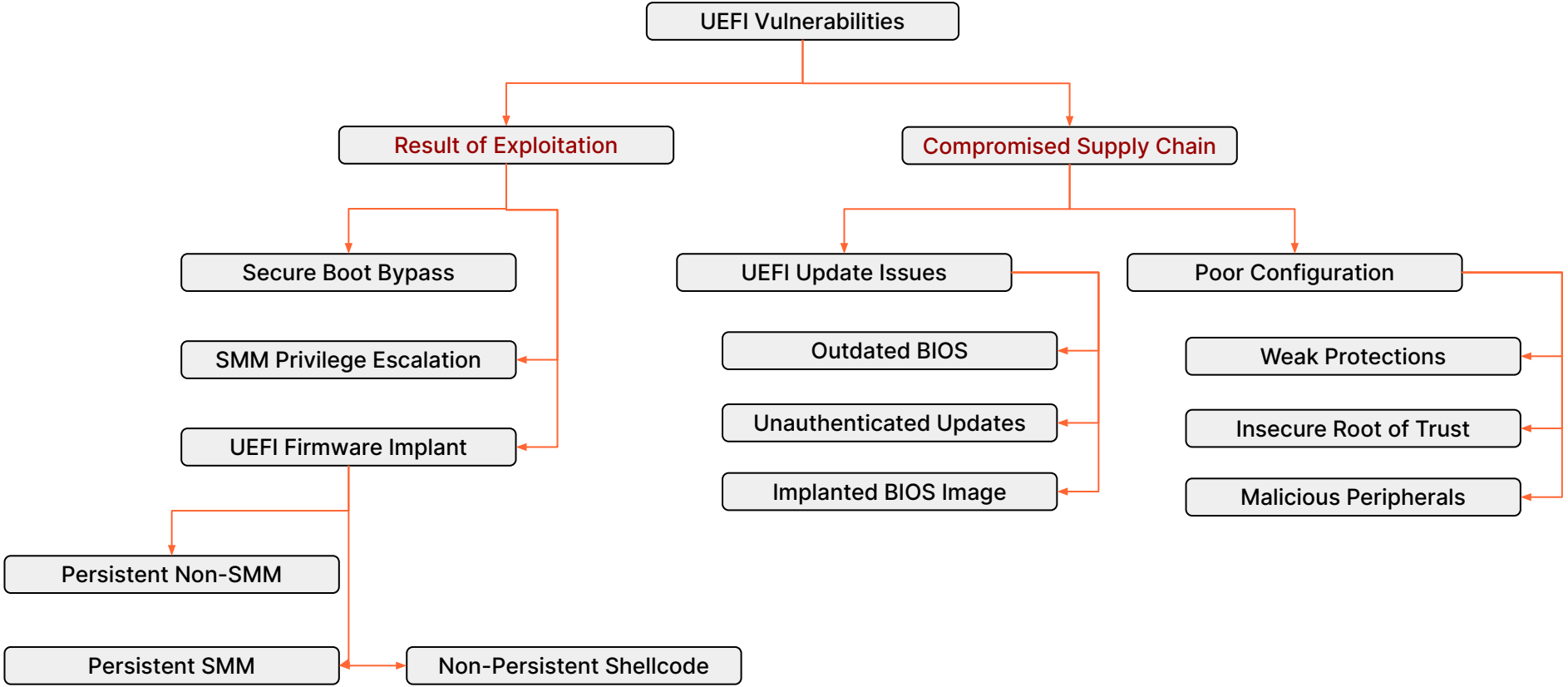






Secure Boot Chain

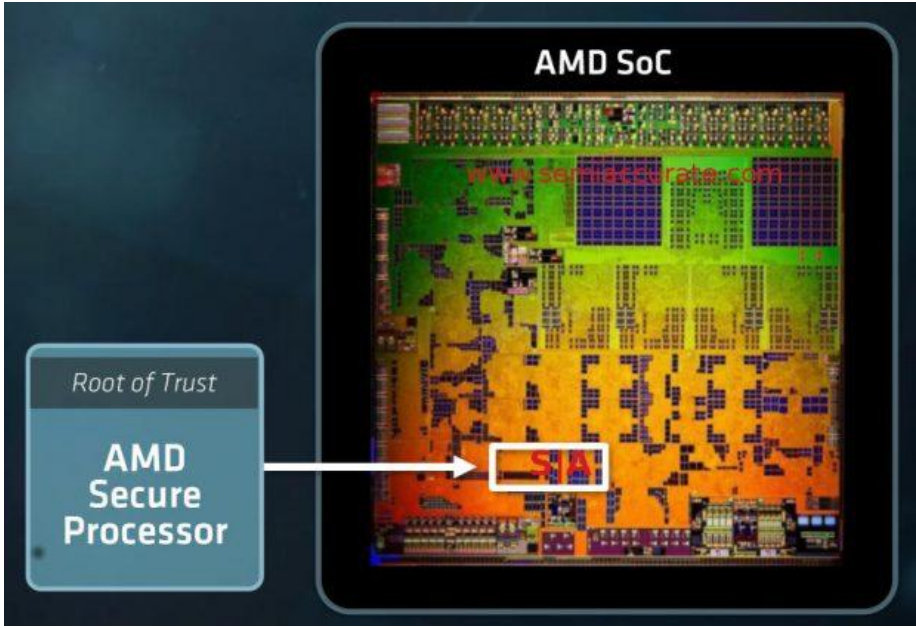


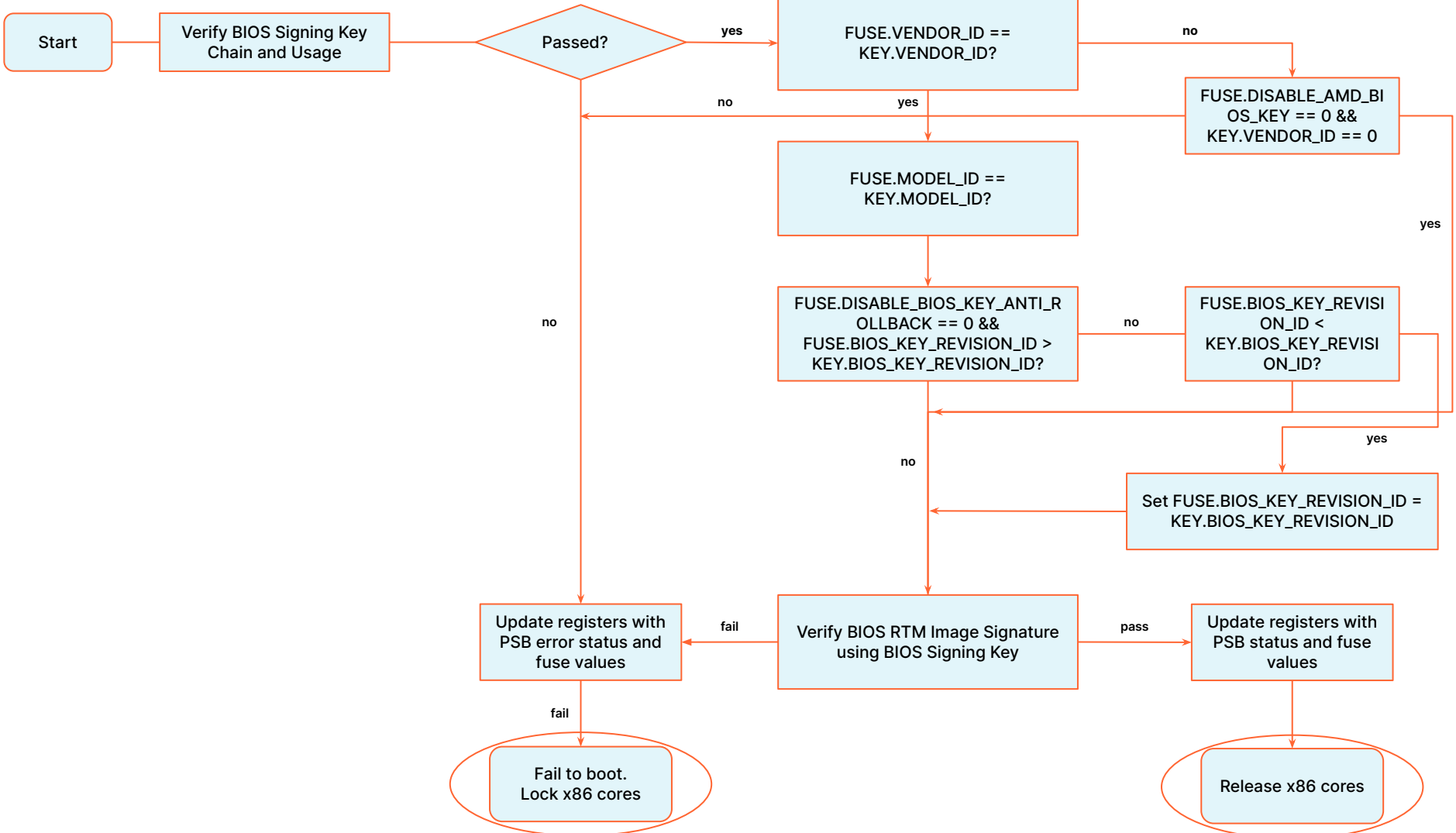

UEFI Vulnerabilities
Result of Exploitation
Compromised Supply Chain
Secure Boot Bypass
SMM Privilege Escalation
UEFI Firmware Implant
Persistent Non-SMM
Persistent SMM
Non-Persistent Shellcode
UEFI Update Issues
Outdated BIOS
Unauthenticated Updates
Implanted BIOS Image
Poor Configuration
Weak Protections
Insecure Root of Trust
Malicious Peripherals

CLOUDFLARE

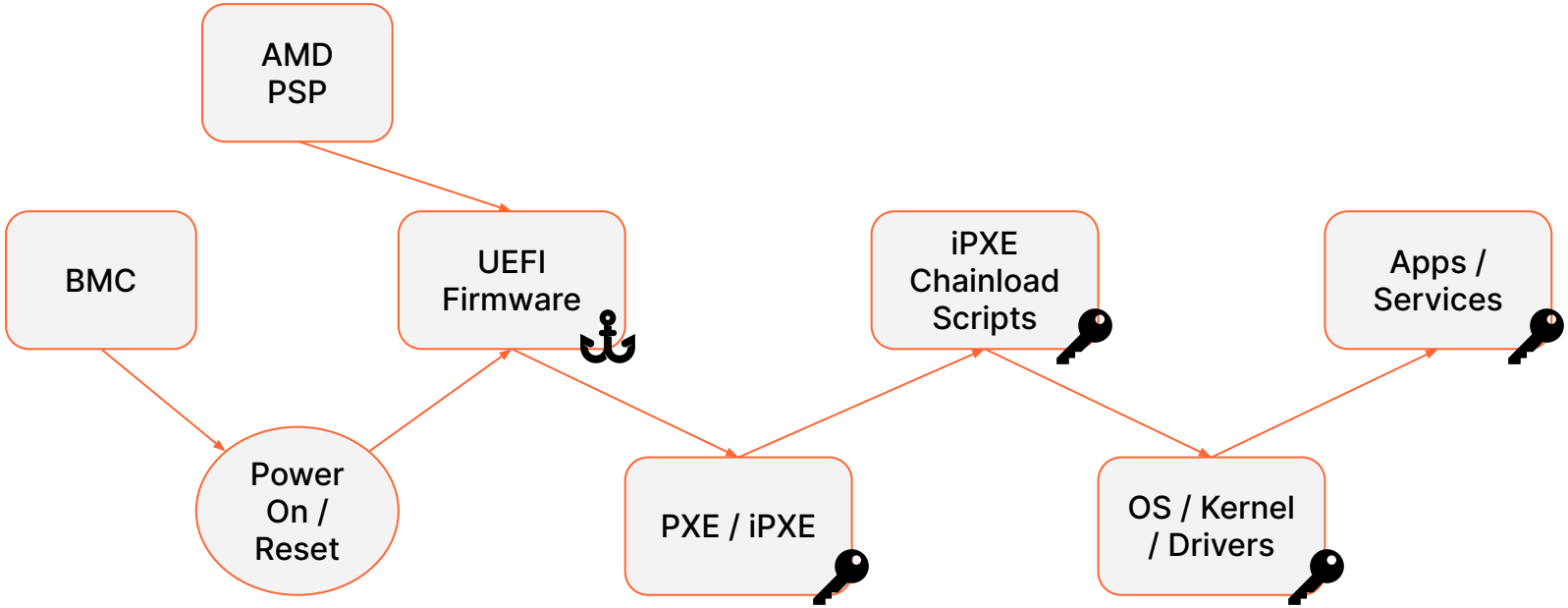
Platform Secure Boot (PSB)

- Authenticates first block of BIOS/UEFI code before releasing x86 CPU from reset.
- Enabled at boot time with PSB-ready FW image.
- PSB is configured using a region of one-time programmable (OTP) fuses, specified for the customer.

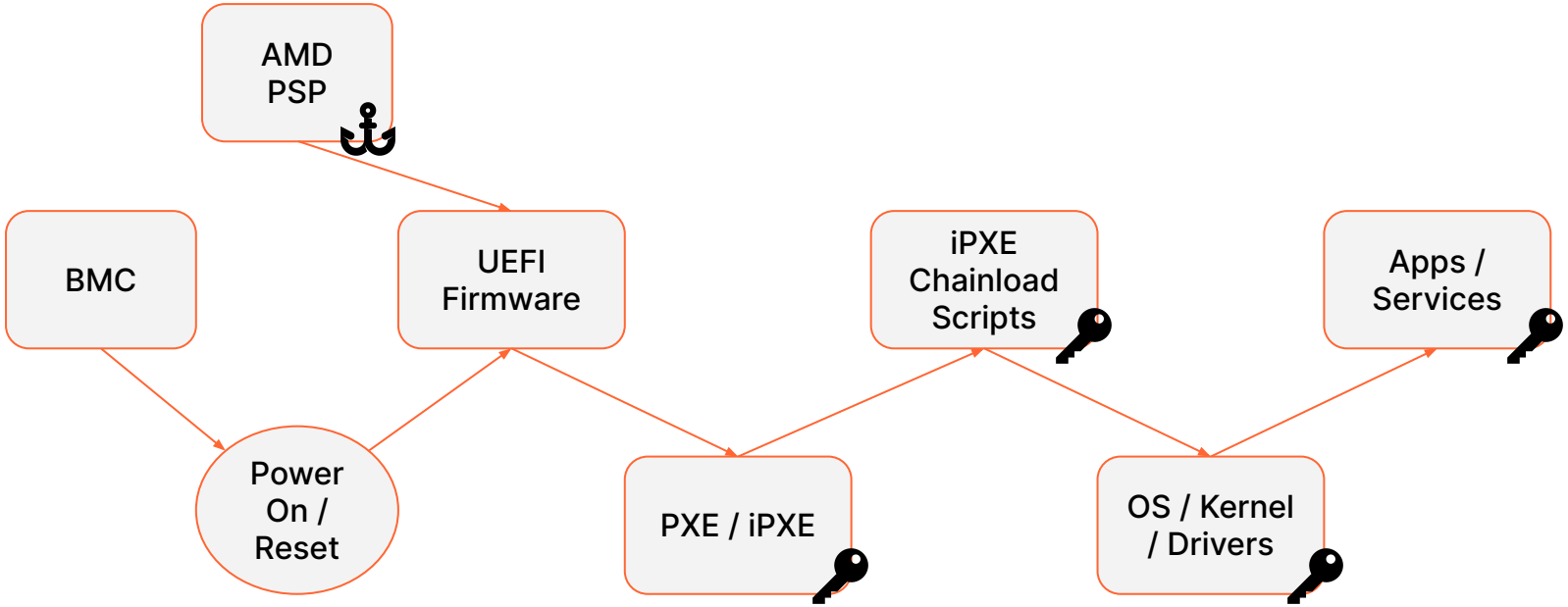



Start
Verify BIOS Signing Key Chain and Usage
Passed?
yes
FUSE.VENDOR_ID == KEY.VENDOR_ID?
no
FUSE.DISABLE_AMD_BIOS_KEY == 0 && KEY.VENDOR_ID == 0
yes
no
yes
FUSE.MODEL_ID == KEY.MODEL_ID?
FUSE.DISABLE_BIOS_KEY_ANTI_ROLLBACK == 0 && FUSE.BIOS_KEY_REVISION_ID > KEY.BIOS_KEY_REVISION_ID?
no
FUSE.BIOS_KEY_REVISION_ID < KEY.BIOS_KEY_REVISION_ID?
no
yes
yes
no
Set FUSE.BIOS_KEY_REVISION_ID = KEY.BIOS_KEY_REVISION_ID
Update registers with PSB error status and fuse values
fail
Verify BIOS RTM Image Signature using BIOS Signing Key
pass
Update registers with PSB status and fuse values
fail
Fail to boot. Lock x86 cores
Release x86 cores

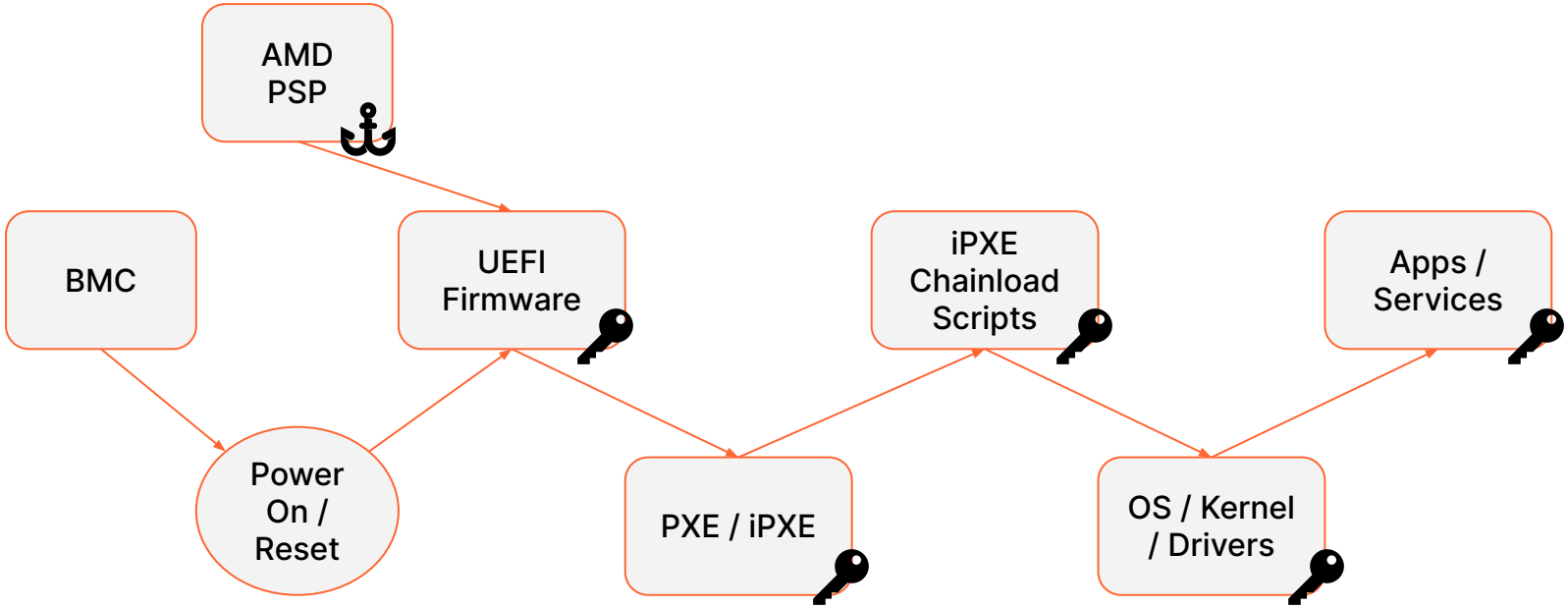
Updated Secure Boot Chain



Updated Secure Boot Chain



Updated Secure Boot Chain



CLOUDFLARE

ARM Secure Boot

Background

Arm Trusted Board Boot Requirements aka "ATF Secure Boot".

How to build a “Chain of Trust” from the first ROM executed (BL1) to “Normal World” firmware (BL33)

System on a Chip (SOC) manufacturer heavily involved in secure boot chain

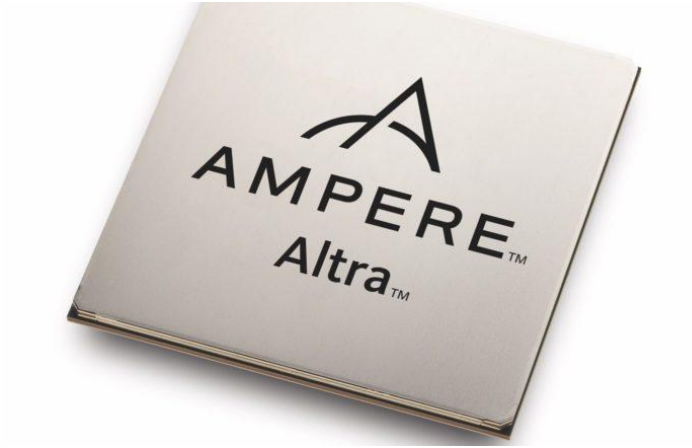
- Requires unique SOC stock keeping unit (SKU) per customer
- SOC manufacturer has end-to-end signing responsibility
- Complicated infrastructure
- Doesn’t scale

≠

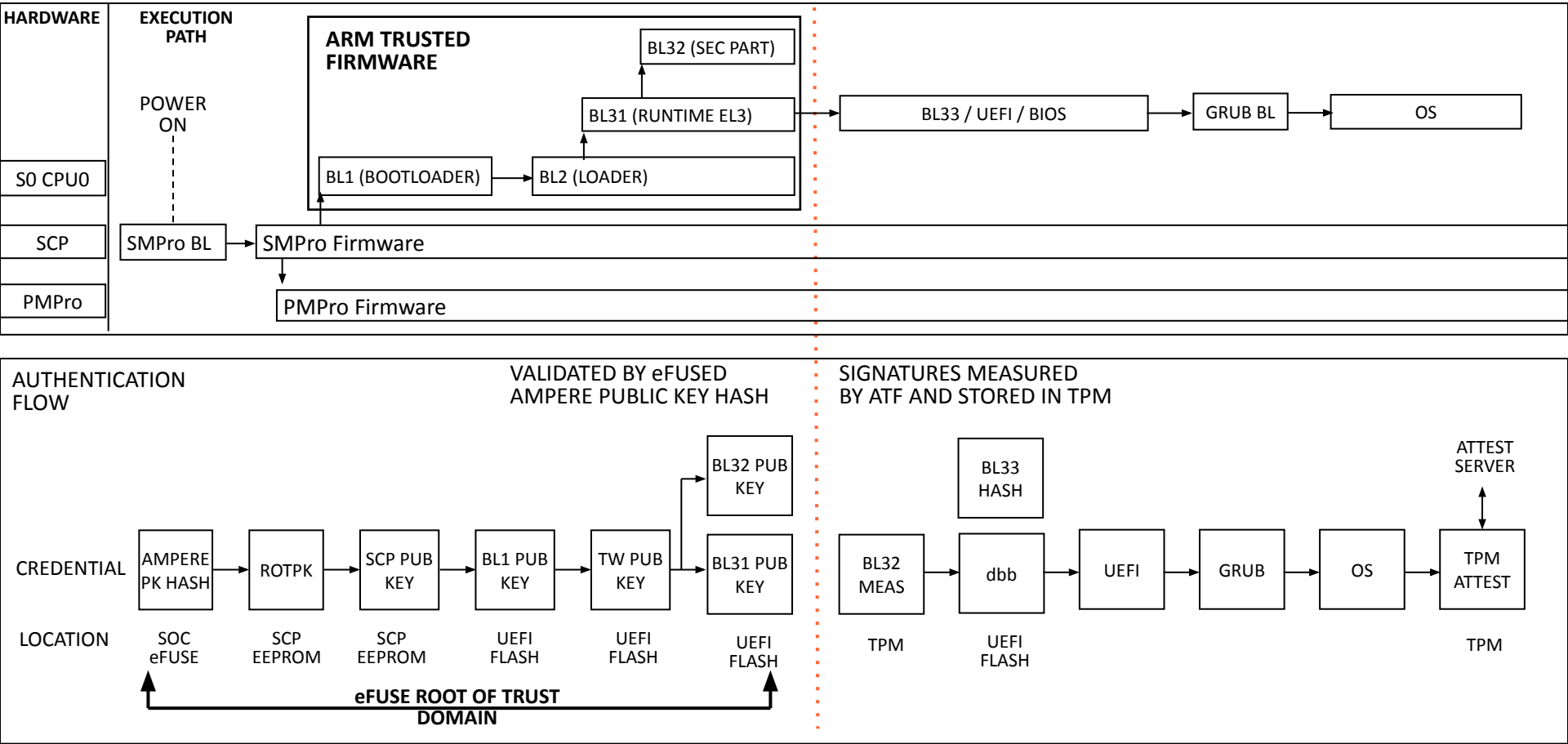
Ampere Computing

CLOUDFLARE

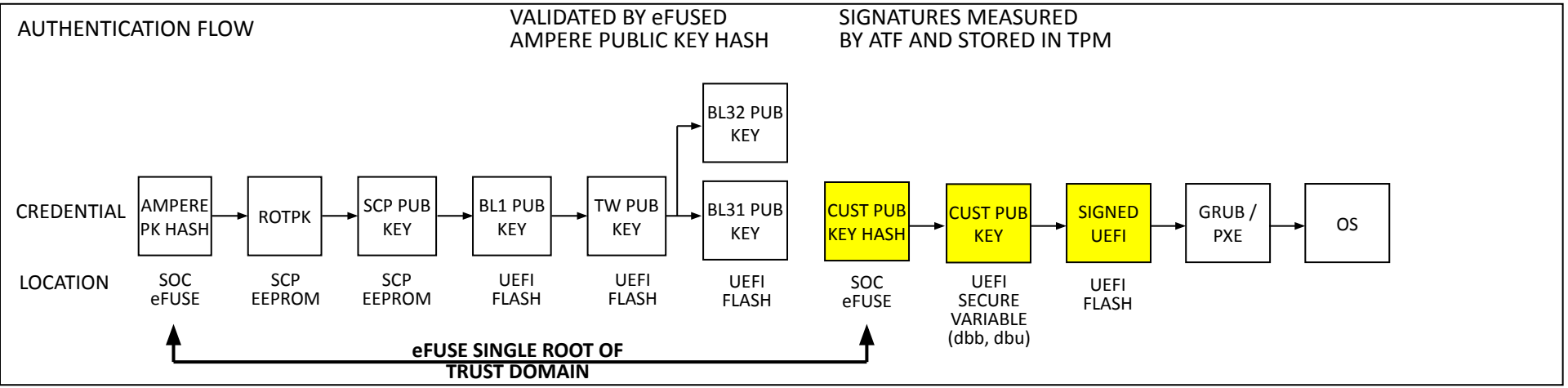
- 128+ core ARM M1 core processor
- ARM V8.2+ extensions
- High memory, I/O, network bandwidth
- Lower TDP than x86



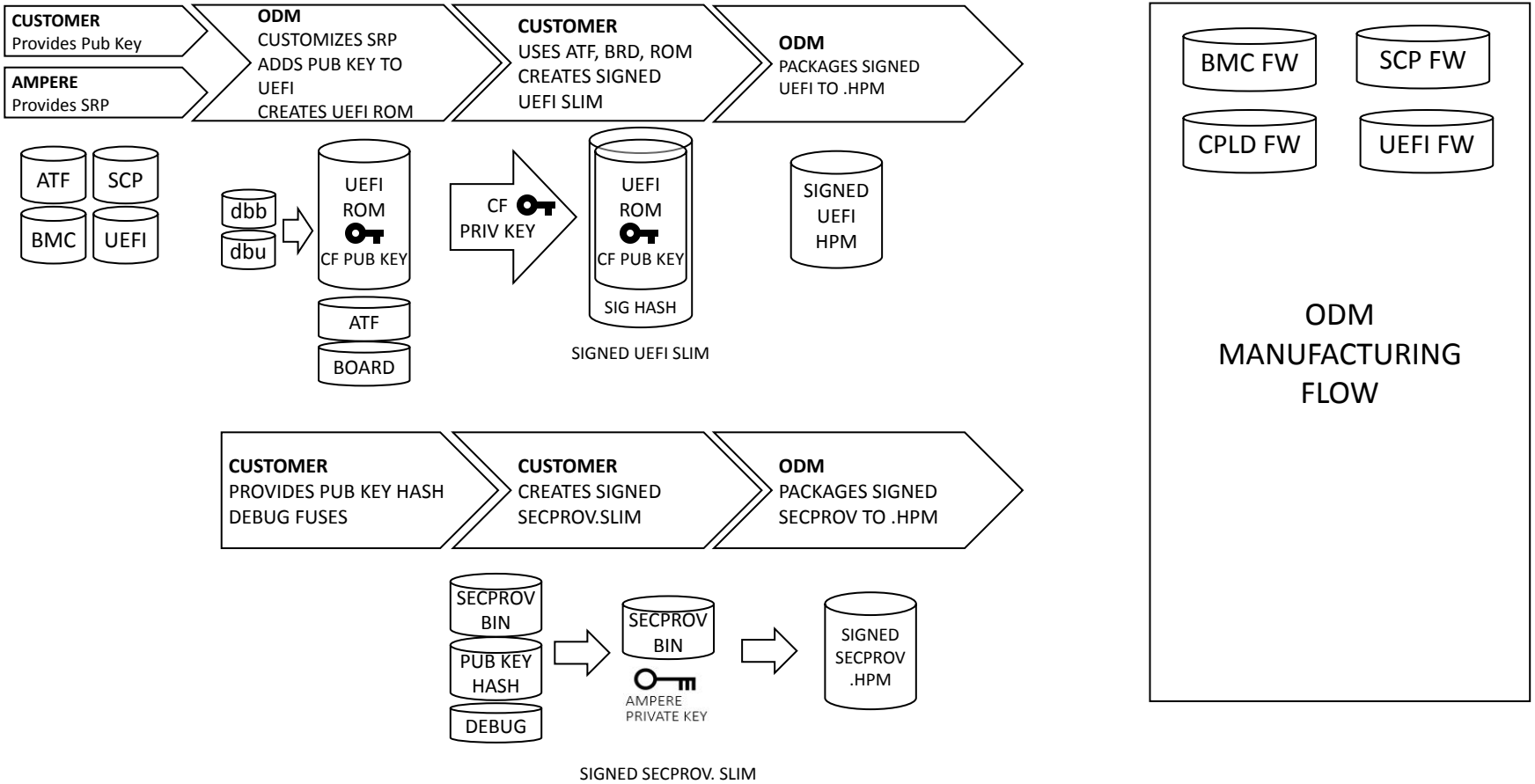
Arm (Ampere) Secure Boot



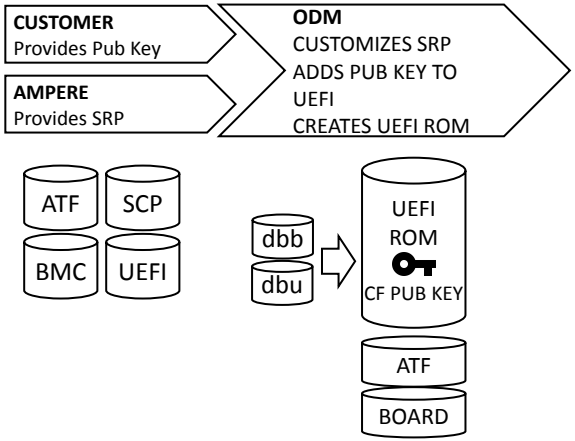
Chain of Trust Revision - Single Domain Secure Boot



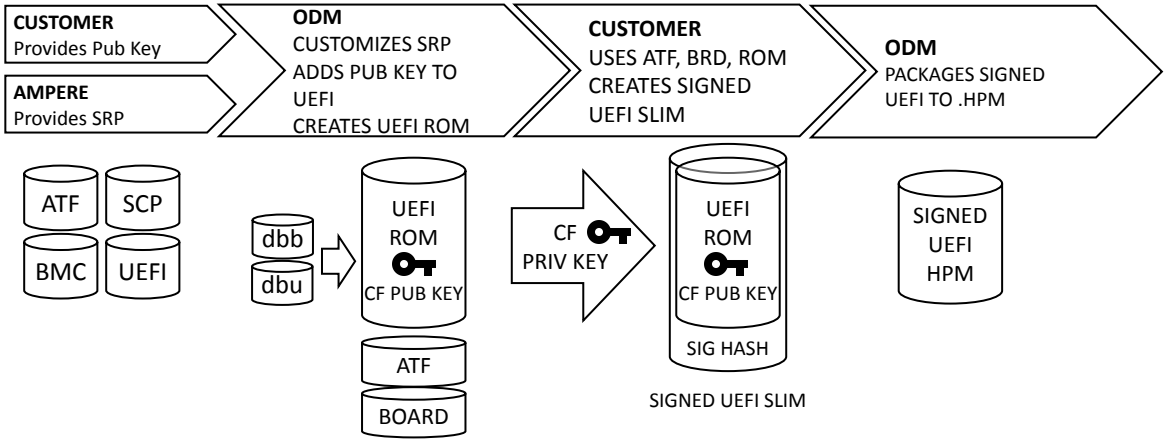
Single Domain Secure Boot (SDSB) Provisioning



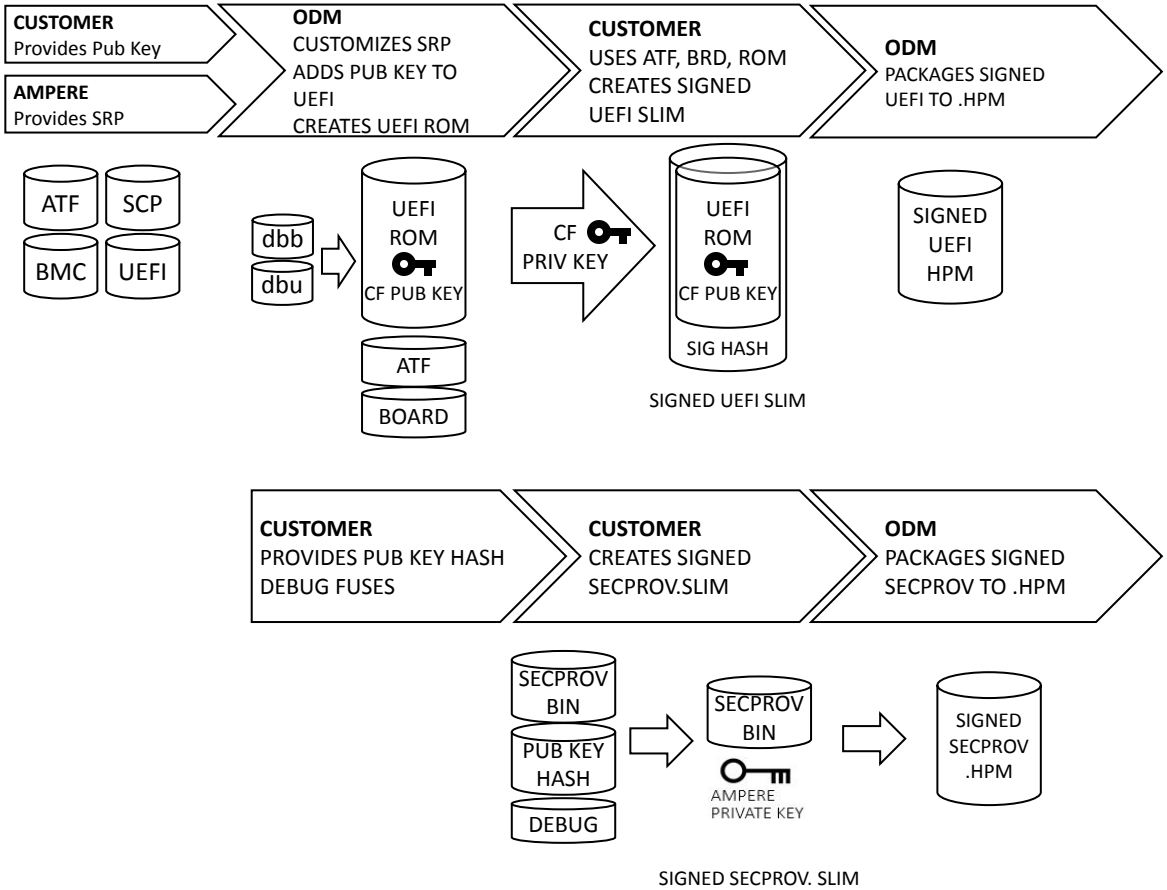
SRP Customization



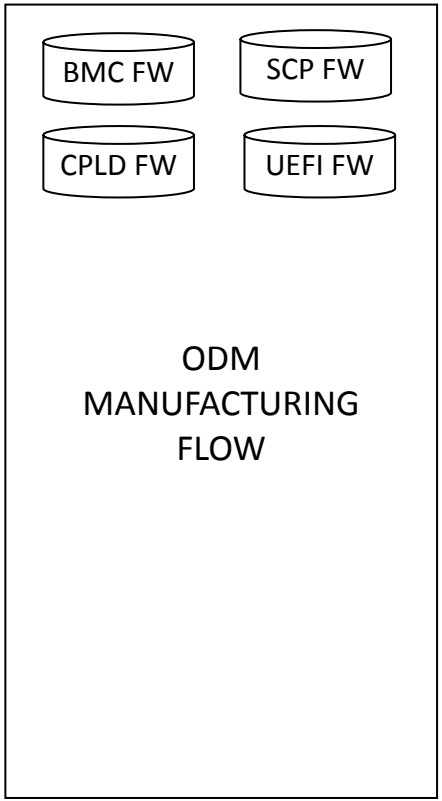
Signed UEFI Firmware

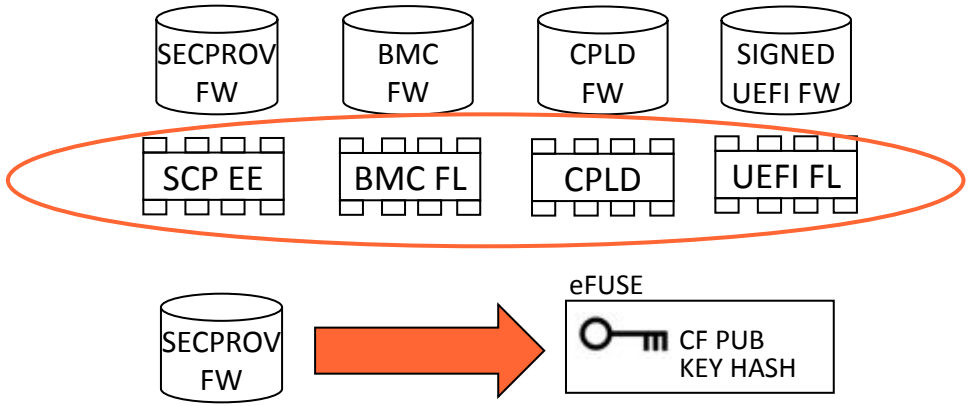


Security Provisioning Firmware

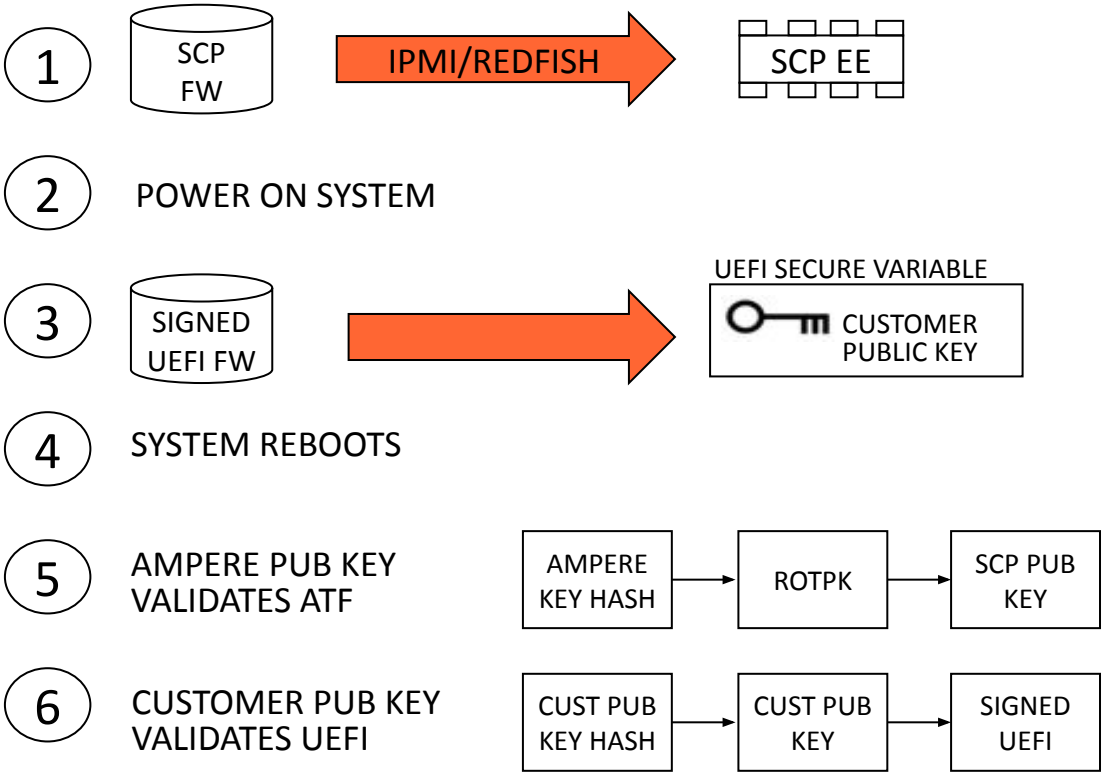


eFuse Key Provisioning

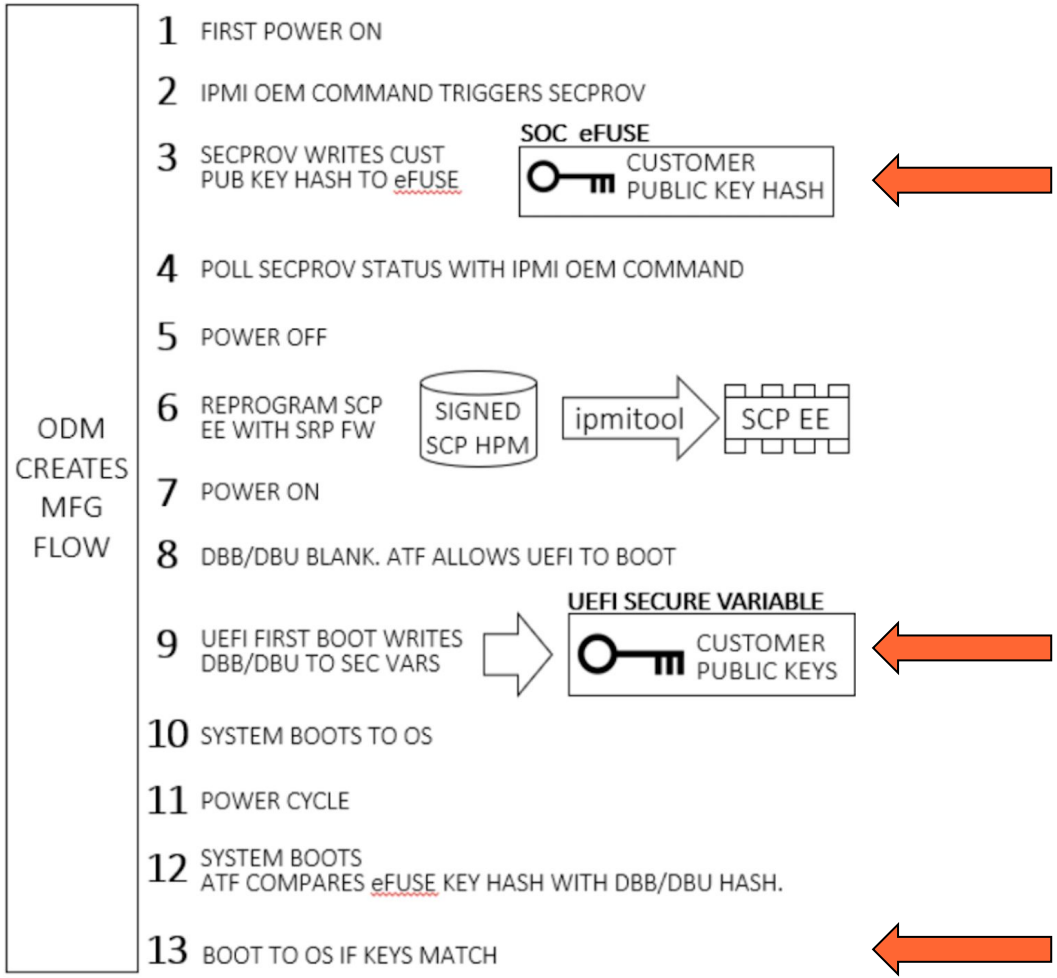




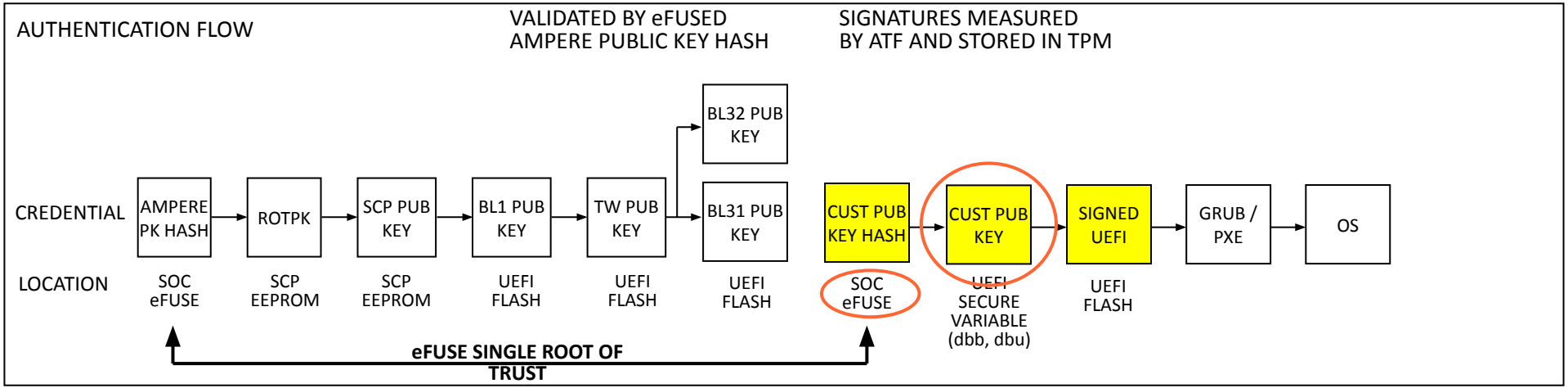
Final Manufacturing Flow



Validation

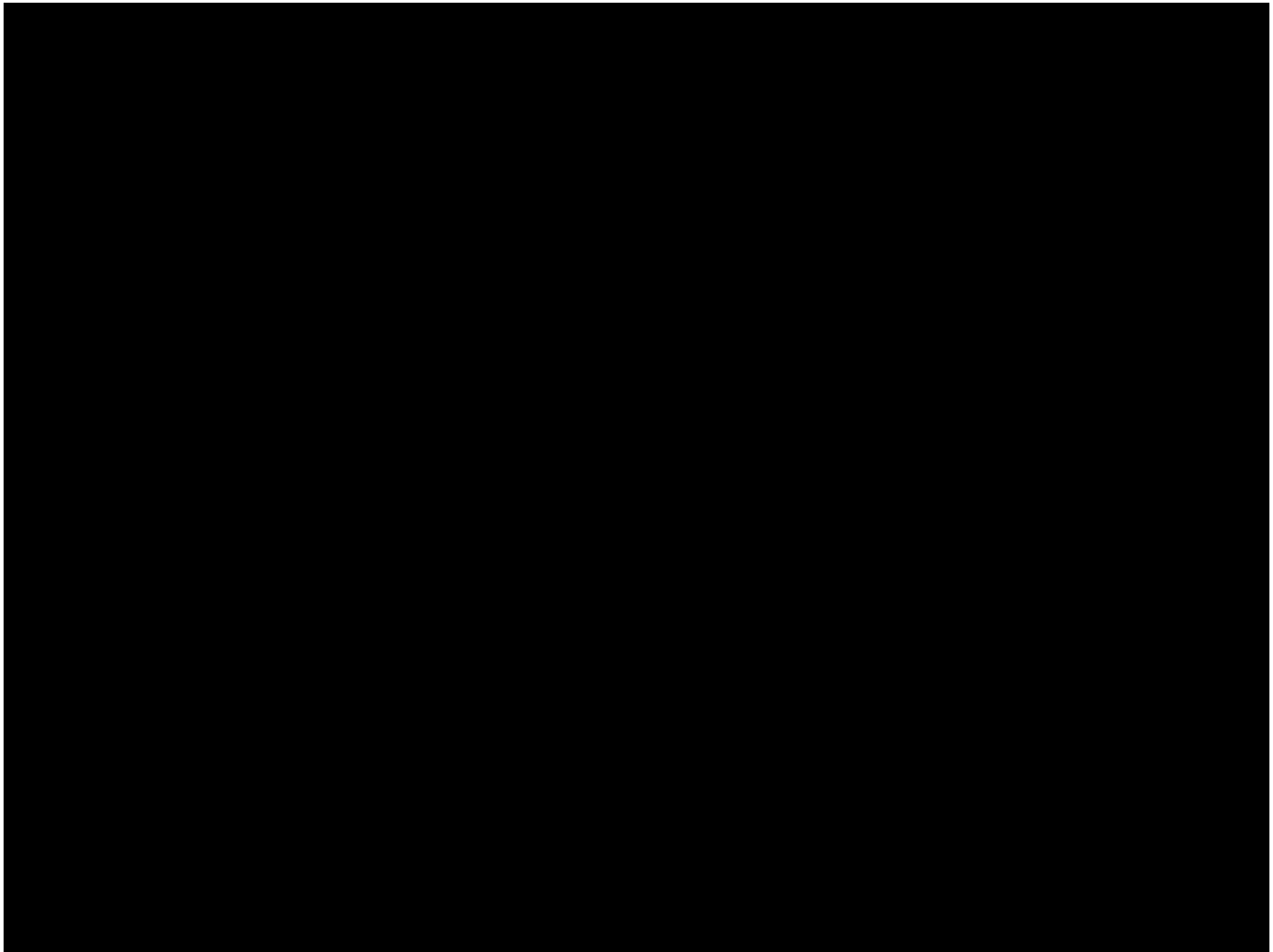

ODM CREATES MFG FLOW
1 FIRST POWER ON
2 IPMI OEM COMMAND TRIGGERS SECPROV
3 SECPROV WRITES CUST PUB KEY HASH TO eFUSE
SOC eFUSE
CUSTOMER PUBLIC KEY HASH
4 POLL SECPROV STATUS WITH IPMI OEM COMMAND
5 POWER OFF
6 REPROGRAM SCP EE WITH SRP FW
SIGNED SCP HPM
ipmitool
SCP EE
7 POWER ON
8 DBB/DBU BLANK. ATF ALLOWS UEFI TO BOOT
9 UEFI FIRST BOOT WRITES DBB/DBU TO SEC VARS
UEFI SECURE VARIABLE
CUSTOMER PUBLIC KEYS
10 SYSTEM BOOTS TO OS
11 POWER CYCLE
12 SYSTEM BOOTS
ATF COMPARES eFUSE KEY HASH WITH DBB/DBU HASH.
13 BOOT TO OS IF KEYS MATCH

UEFI Authentication



CLOUDFLARE

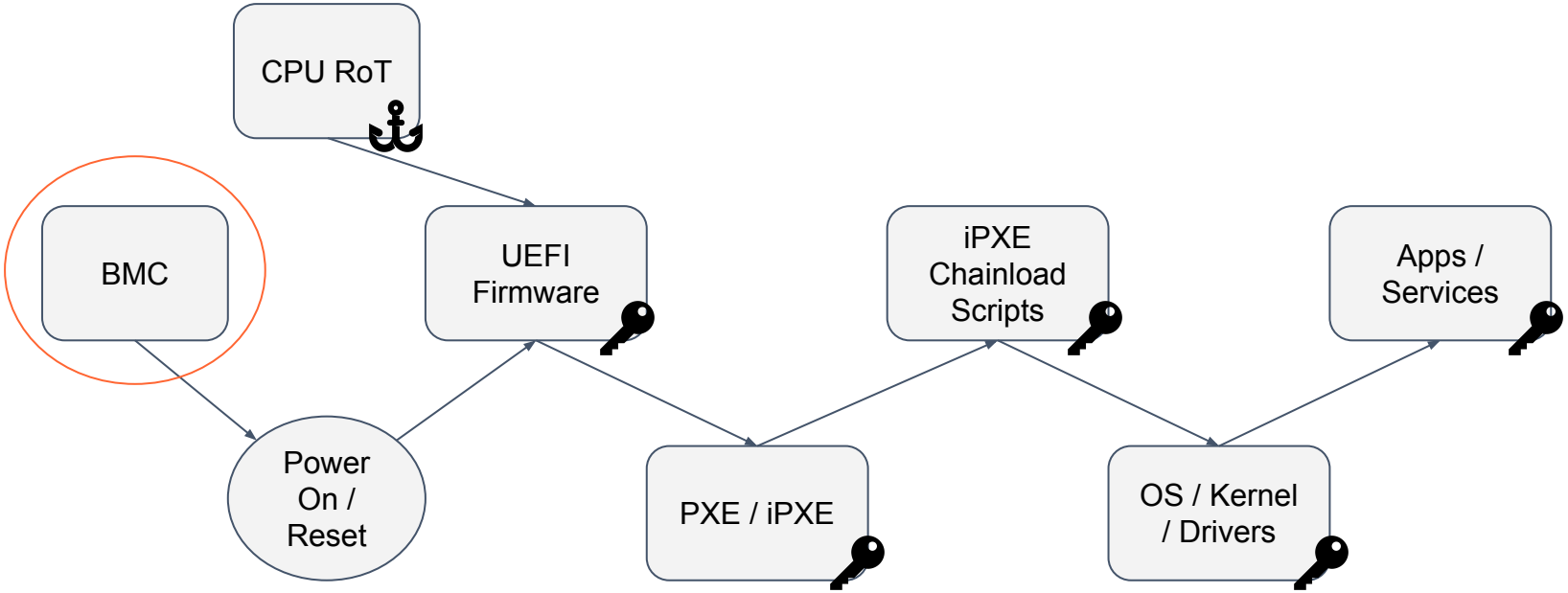
Demo



CLOUDFLARE

BMC Protection

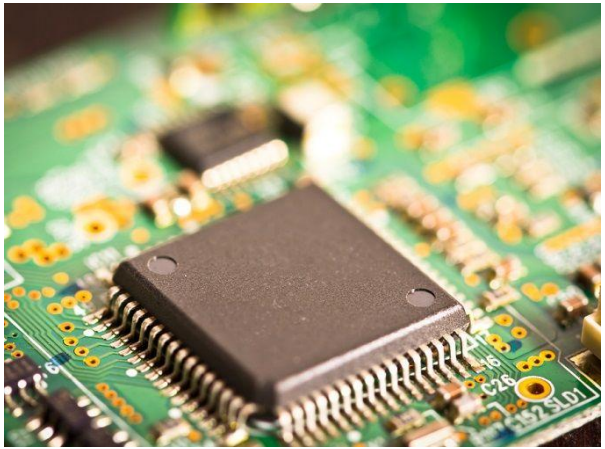
CPU-based Root of Trust



Why Attack a BMC?

CLOUDFLARE

- Highly privileged access to host
- Network accessible
- Connected to both host and management network
- Persistence independent from host
- Poor firmware security history
    - https://blog.cloudflare.com/bmc-vuln/



CLOUDFLARE

Future

Security Co-Processors

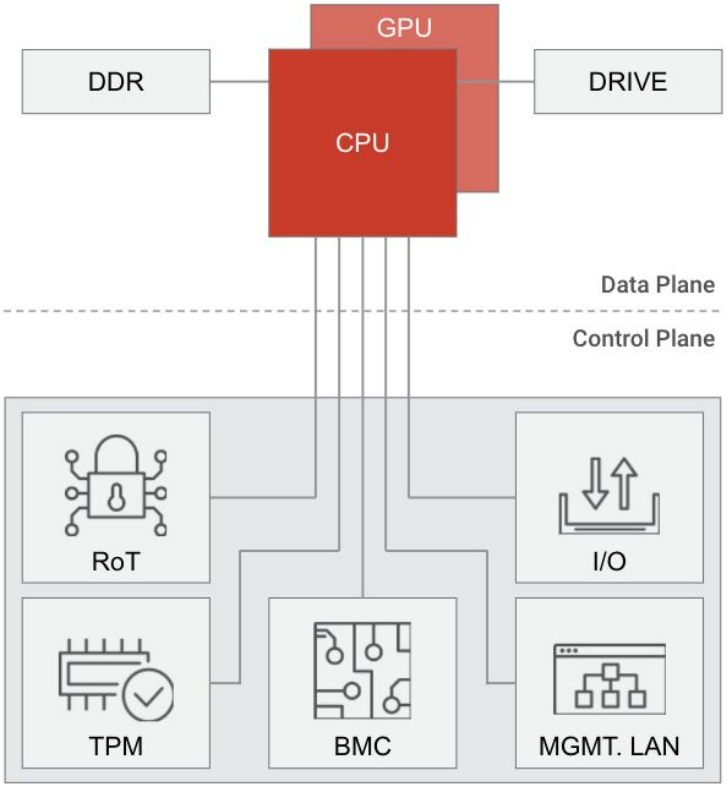
CLOUDFLARE

AXIADO

OPEN Compute Project

Kameleon

- Platform Secure Boot
- Firmware integrity
- PUF-based identity
- Peripheral attestation
- Key transition



blog.cloudflare.com

CLOUDFLARE

Thank you

				Invasive Debug		Non-Invasive Debug	
SPIDEN	**DBGEN**	**SPNIDEN**	**NIDEN**	**Secure**	**Not Secure**	**Secure**	**Not Secure**
0	0	0	0	N	N	N	N
0	0	0	1	N	N	N	Y
0	0	1	1	N	N	Y	Y
0	1	0	1	N	Y	N	Y
0	1	1	1	N	Y	Y	Y
1	1	1	1	Y	Y	Y	Y