DEVELOPING BOOT SOLUTIONS FOR INTEL IOT UNIQUE USE CASES

Yah-Wen Ho

Senior BIOS & Bootloader Lead

Intel Internet of Things Group (IoTG)

PROBLEM STATEMENT

The Internet of Things (IoT) has a wide variety of use cases, and current bootloader solutions do not properly address all the requirements:

- Ease of implementation
- Security
- Extensible design
- Scaling across verticals
- Open source with permissive licensing
- Leverages Intel® Firmware Support Package (Intel® FSP)

SLIM BOOTLOADER

(SBL)

SLIM BOOTLOADER VALUE PROP

Designed to enable new experiences and customer centric innovation for a variety of IOT use cases

IoT Use Cases

HIGHLY ADAPTABLE, CUSTOMIZABLE & IOT FOCUSED

Slim Bootloader

Fast Boot

FASTER

COMPARED TO PREVIOUS INTEL BOOTLOADER SOLUTIONS

APL – 420 ms[1]

Security

INTEGRATED

VERIFIED BOOT
MEASURED BOOT
FW UPDATE

Permissive License

BSD

ALLOWS PROPRIETARY CUSTOMIZATIONS

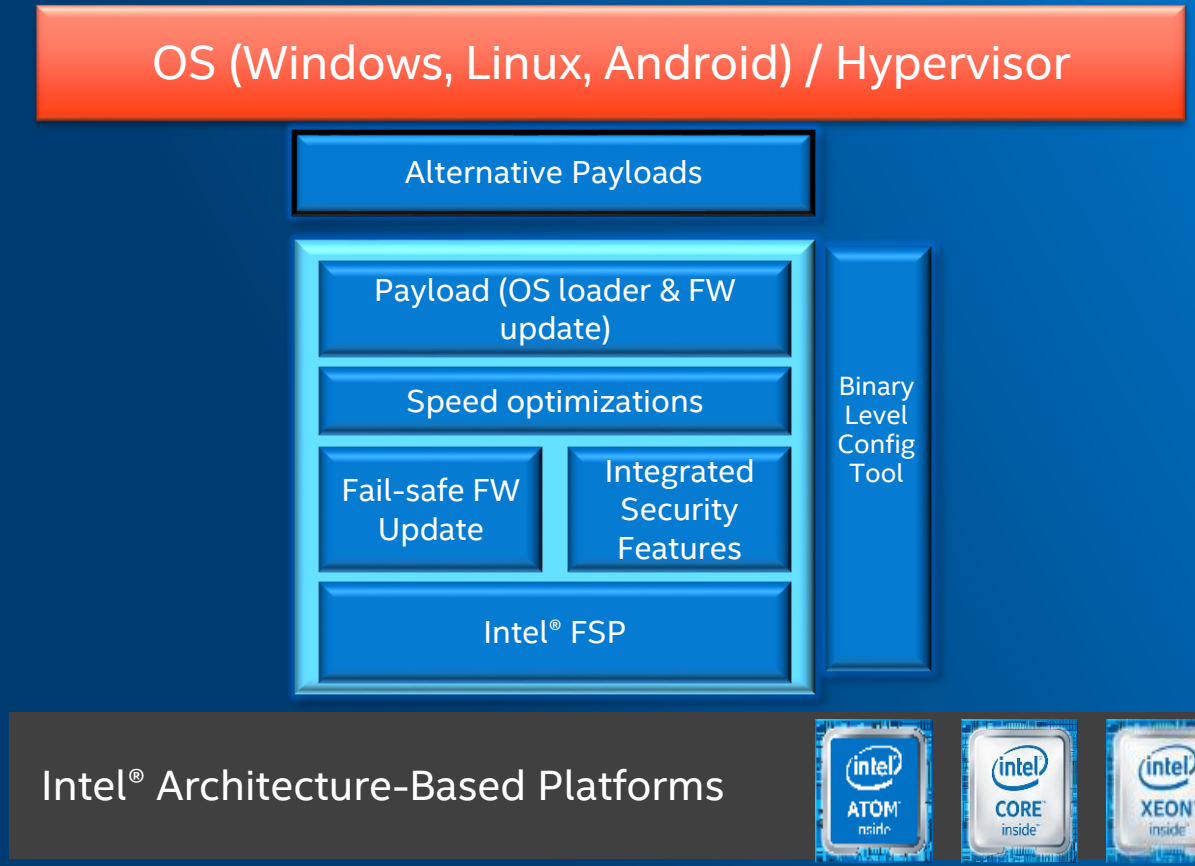
Ecosystem

WIDE

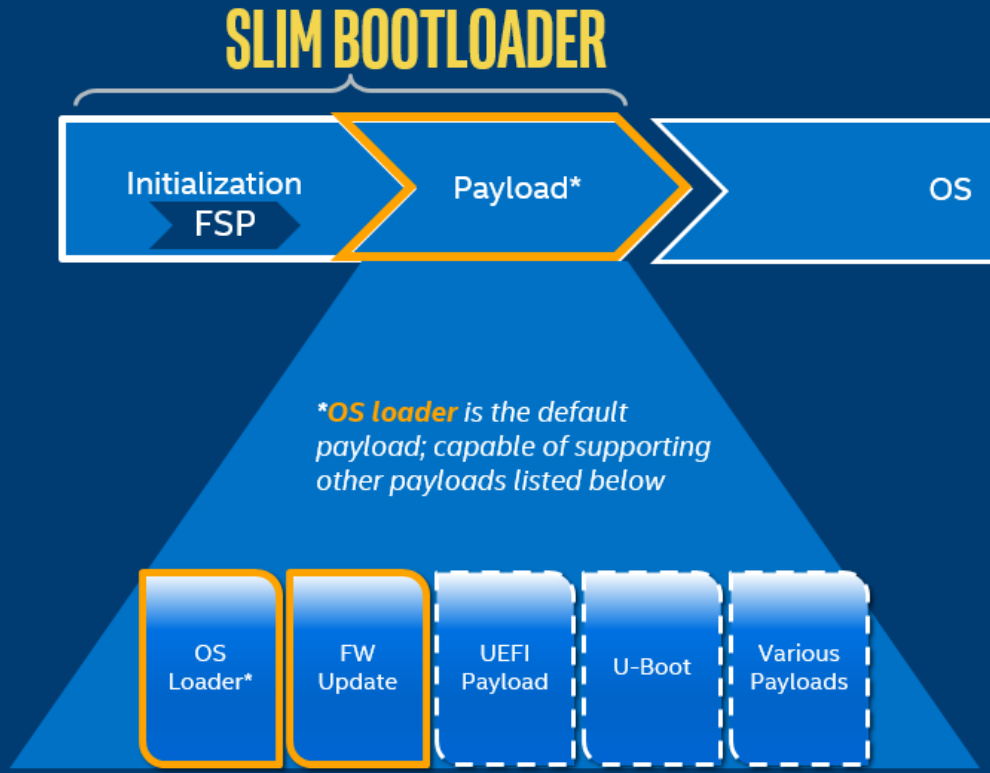
ENABLED FOR CUSTOMIZATION AND MAINTENANCE

1: Up to 420ms fast claim based on APL Leaf Hill REVD board running SBL on Atom™ Processor E3950 running at 1.6GHz with HT enabled, Turbo enabled , LPDDR4 8GB, 64G eMMC 5.1. FSP version MR5 from https://github.com/IntelFsp/FSP.git branch ApolloLoake, revision a57c66616e78b471515a1e1862796bf61d3824d8. Compiler: Microsoft Visual Studio professional 2013, Python2.7.10, NASM version 2.12.01rc2 compiled on Mar 7 2016, Intel ASL+ Optimizing Compiler version 20160422-32. Measured from CPU Reset vector to OS entry point. Includes (OS Loader) payload boot time.

SLIM BOOTLOADER ARCHITECTURE



PAYLOAD



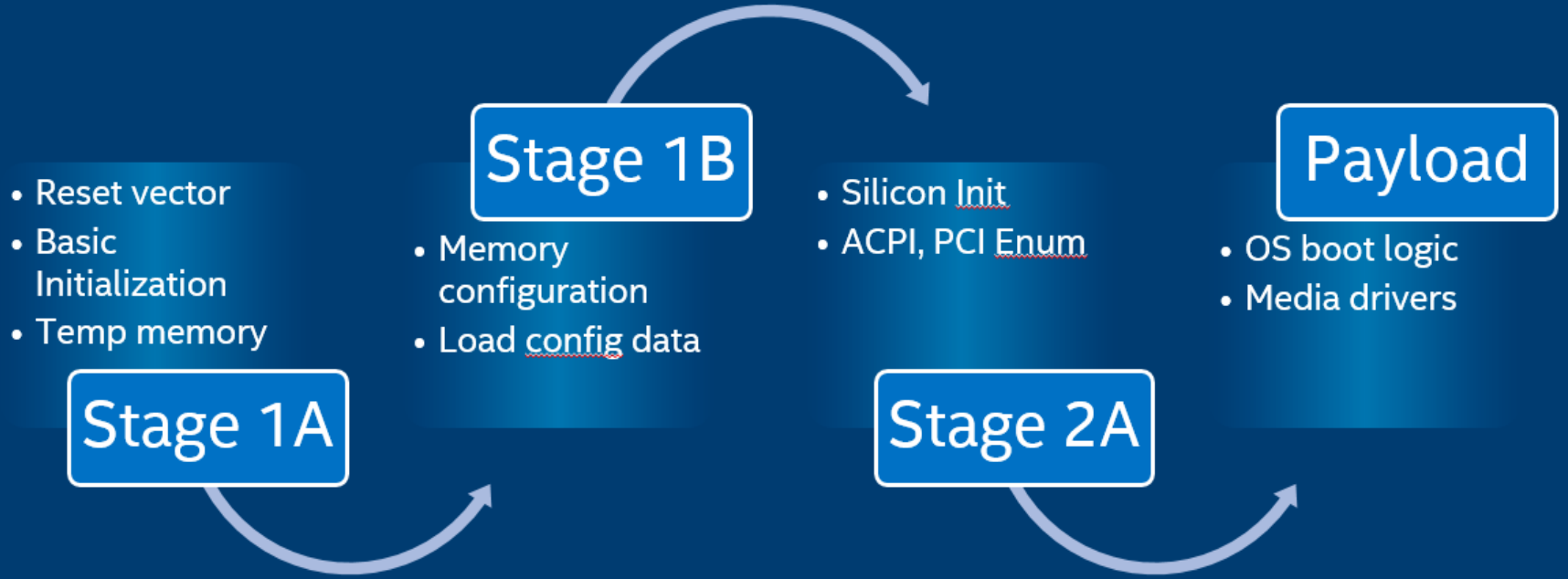
SBL: Board and silicon initialization, including resource allocation, GPIO, ACPI, etc.

Payloads: Generic media drivers, custom features, OS specific loading protocols, etc.

OS Loader: Optimized payload specifically for IOT use cases

FW Update: Power fail-safe, fault tolerant, secure firmware update

BOOT LIFE CYCLE WITH SBL



ENABLED PRODUCTS AS DEVELOPMENT VEHICLE

Intel® Atom™ E3900 Series (Available now)

(formerly known as Apollo Lake)

Boards Supported:

- Aaeon UP Squared
- Intel E3900 Series Customer Reference Boards:
  - Leaf Hill
  - Oxbow Hill
  - Juniper Hill

More to come!

CALL TO ACTION

- Try out Slim Bootloader
- Intel appreciates your valuable feedback and comments
- Participate and contribute to the Slim Bootloader open source community

Links:

- Slim Bootloader web page: intel.com/sbl
- Source: github.com/slimbootloader
- Slim Bootloader mailing list: lists.01.org/mailman/listinfo/sbl-devel


intel®
experience
what's inside™