presented by

"Last Mile" Barriers to Removing Legacy BIOS

Fall 2017 UEFI Plugfest

October 30 – November 3, 2017

Presented by Brian Richardson (Intel Corporation)

Agenda

- What is the “Last Mile”?
- Wait … we’re still talking about BIOS? Why?
- Advantages using UEFI Class 3
- Areas of Focus
- Call to Action

"Last Mile" Barriers to Removing Legacy BIOS

What is the “Last Mile”?

Last mile: the last step of delivering infrastructure to customers…

"Last Mile" Barriers to Removing Legacy BIOS

Wait … we're still talking about BIOS? Why?

Wait … we’re still talking about BIOS? Why?

There is still a reliance on 16-bit BIOS via the Compatibility Support Module (CSM)

1. People still use software that depends on 16-bit BIOS runtime
2. Power-users “disable UEFI” to bypass secure boot or setup multi-OS boot

Reminder: UEFI System Classes

UEFI Class 0

- Legacy BIOS
- No UEFI or UEFI PI interfaces

UEFI Class 1

- Uses UEFI/PI interfaces
- Runtime exposes only legacy BIOS runtime interfaces

UEFI Class 2

- Uses UEFI/PI interfaces
- Runtime exposes UEFI and legacy BIOS interfaces

UEFI Class 3

- Uses UEFI/PI interfaces
- Runtime exposes only UEFI interfaces

… and there's one "unspoken class"

UEFI Class 0

- Legacy BIOS
- No UEFI or UEFI PI interfaces

UEFI Class 1

- Uses UEFI/PI interfaces
- Runtime exposes only legacy BIOS runtime interfaces

es

FI and

s

Enabling secure boot essentially creates another UEFI Class

UEFI Class 3+

- Uses UEFI/PI interfaces
- Runtime exposes only UEFI interfaces
- **UEFI Secure Boot ON**

Why are BIOS & CSM still a thing?

- One specific tool doesn’t work with UEFI, so users turn on the CSM as a fix
  (as we say in Georgia, duct tape is cheaper than welding)

- Some users blame UEFI or Secure Boot whenever something doesn’t work
  (if you don’t believe me, search for “UEFI” on Twitter)

Issues Relying on 16-bit Legacy

Security Risks

- No standards for secure boot or signed code execution

Complicates Validation

- Requires two validation paths (CSM ON & CSM OFF)

Supporting Modern Technology

- New technologies may not provide backward compatibility

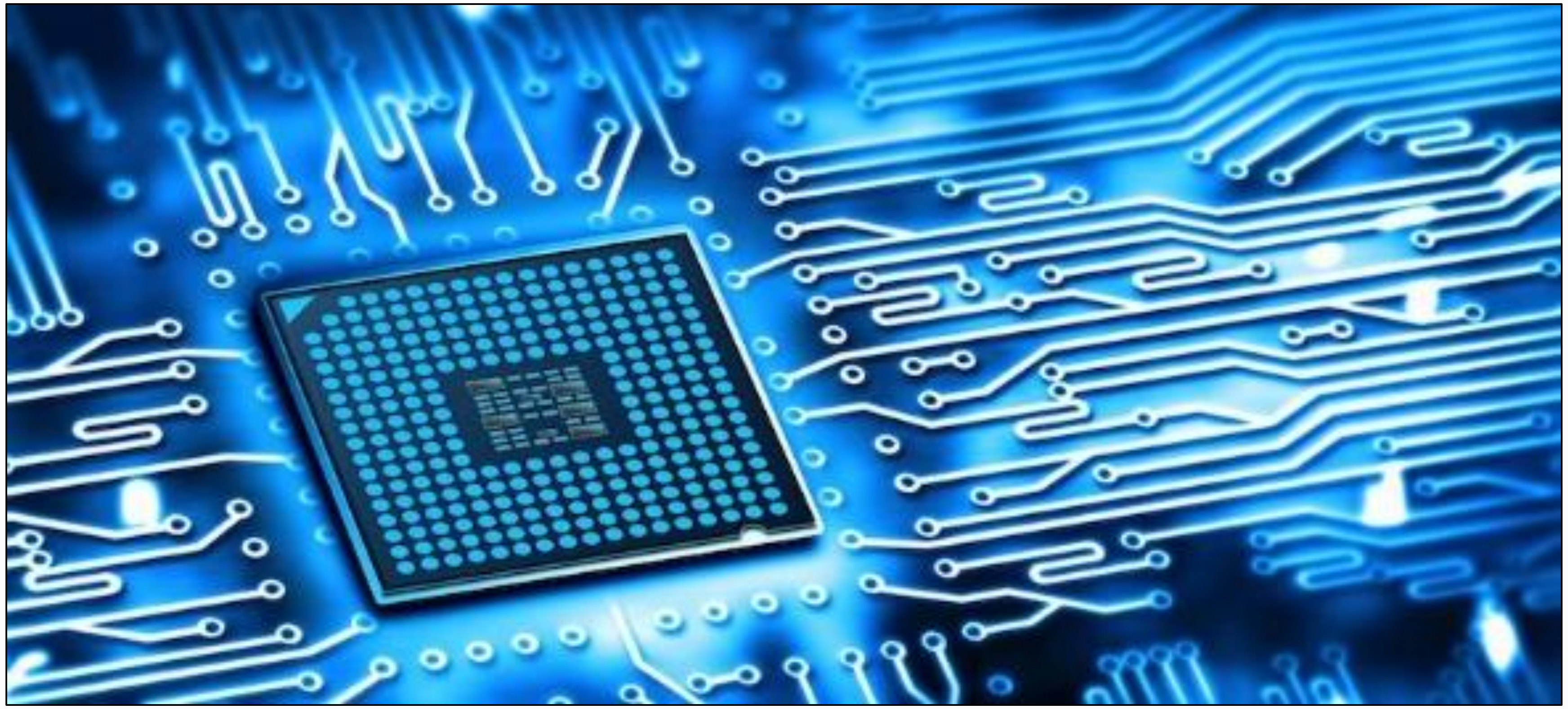
What is the “last ~~mile~~ km” for UEFI?

Retiring legacy code and related processes

- Tools (disk duplication, testing, update)
- Network Boot (PXE) to legacy images

Remove user motivations to stick with BIOS

- Improve experience with UEFI Secure Boot
- Promote enhanced UEFI features (HTTPS Boot, OS Recovery, Signed Capsule, …)



"Last Mile" Barriers to Removing Legacy BIOS

Advantages using UEFI Class 3

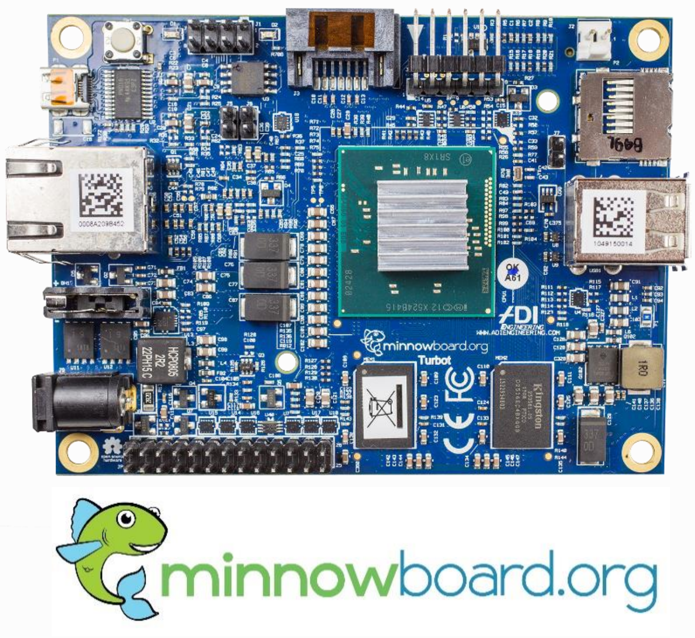
Advantages using UEFI Class 3

- Smaller code size (ROM & OpROM)
- Smaller validation/support footprint
- Encourage use of new technologies

Industry is moving away from CSM

Many Intel Architecture platforms are UEFI Class 3/3+ out of the box

- Many platforms with CSM (UEFI Class 2) have it disabled by default (required when UEFI Secure Boot is enabled)
- Now mandated for specific platforms
- See ‘Security requirements’ on “UEFI requirements for Windows editions on SoC platforms” @ microsoft.com



Intel is deprecating legacy support

Intel is removing legacy BIOS support from client & data center platforms by 2020

- Platforms will be strictly UEFI Class 3
- No 16-bit OpROM (VGA, LAN, Storage)

This will break any customer process that depends on “disabling UEFI” (“CSM ON”)

"Last Mile" Barriers to Removing Legacy BIOS

Areas of Focus

Areas of Focus

- Improve user experience with UEFI Secure Boot (OS install, tools, recovery)
- Eliminate components with no UEFI support
- Remove DOS/BIOS dependencies from manufacturing/maintenance tools
- Educate customers on migrating network boot to UEFI (PXE & HTTPS)

Areas of Focus

- Improve user experience with UEFI Secure Boot (OS install, tools, recovery)
- Eliminate components with no UEFI support

This is the typical consumer scenario, and the most restrictive from a validation standpoint. So…

- Validate your tools with secure boot on
- Customers shouldn’t have to disable secure boot or enable CSM to solve common recovery problems

Areas of Focus

- Improve user experience with UEFI Secure Boot (OS install, tools, recovery)
- Eliminate components with no UEFI support
- Remove DOS/BIOS dependencies from

It’s a supply chain problem… *wait, we’re the supply chain!*

- Drivers, peripherals, and utilities work without CSM
- No DOS requirements for pre-OS validation/tools (try UEFI Shell or Python)

Areas of Focus

- Ir cure B
- Eliminate components with no UEFI support

No DOS requirements for pre-OS validation or maintenance tools (try UEFI Shell or Python)

- Remove DOS/BIOS dependencies from manufacturing/maintenance tools

Can you run manufacturing tests with UEFI Secure Boot enabled (UEFI Class 3+)?

- Educate customers on migrating network boot to UEFI

Areas of Focus

- Promote improved functionality powered by UEFI (i.e. why are HTTPS & OS Recovery awesome?)
- Remove our customer’s incentives to stick with outdated tools that require DOS & BIOS

- Remove DOS/BIOS dependencies from manufacturing/maintenance tools

- Educate customers on migrating network boot to UEFI (PXE & HTTPS)

"Last Mile" Barriers to Removing Legacy BIOS

Call to Action

Call to Action

- Many UEFI platforms still enable legacy BIOS compatibility using CSM
- CSM expose security issues and delays 100% migration to UEFI
- Many modern features have no equivalent legacy functionality and require booting in “UEFI mode”
- Intel is planning to deprecate legacy compatibility by 2020, and is working with partners on a smooth industry transition

Thanks for attending the Fall 2017 UEFI Plugfest

For more information on the UEFI Forum and UEFI Specifications, visit http://www.uefi.org

presented by