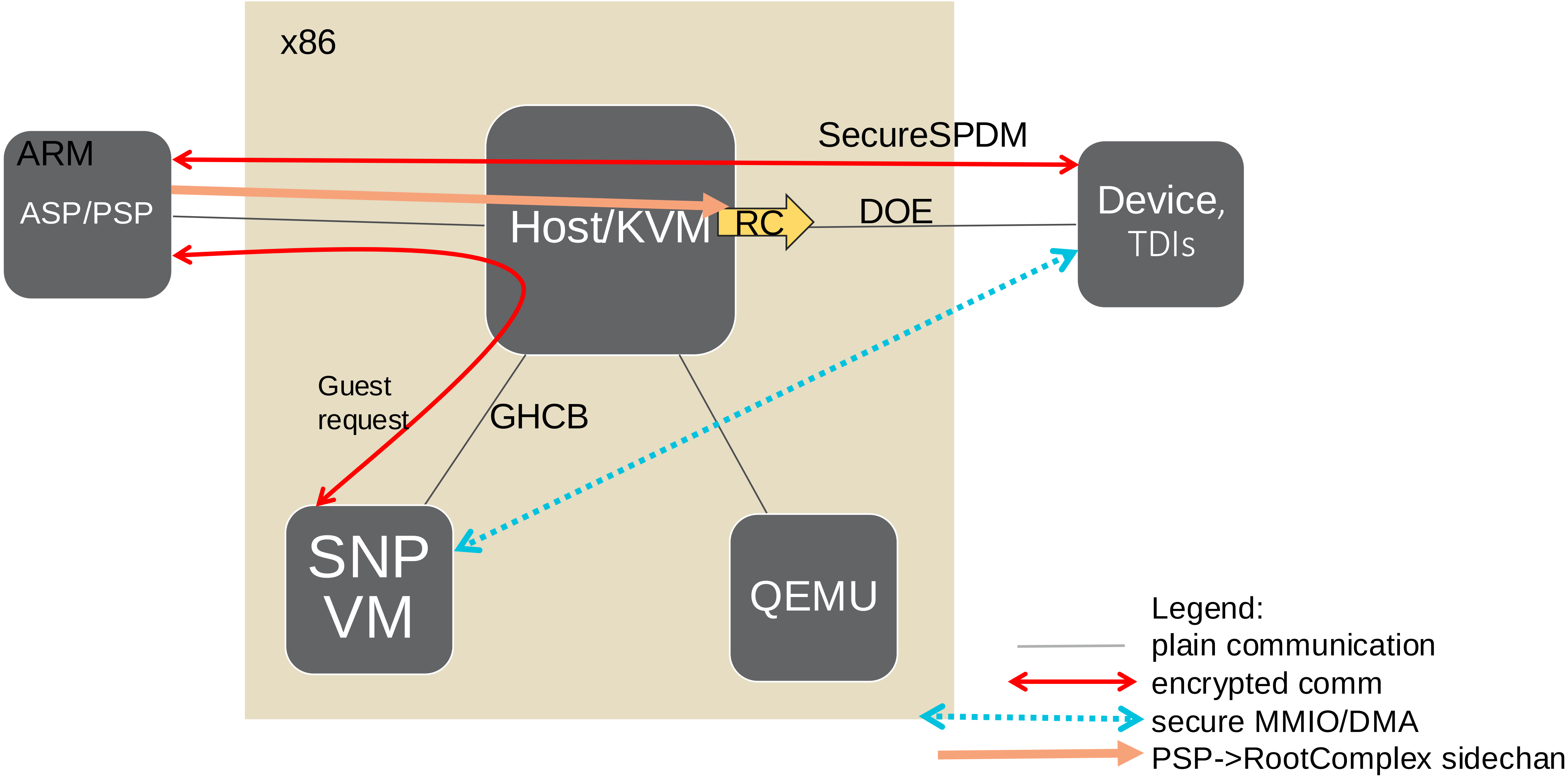
SEV TIO

Alexey Kardashevskiy, AMD Far East

Linux Plumbers Conference 2024

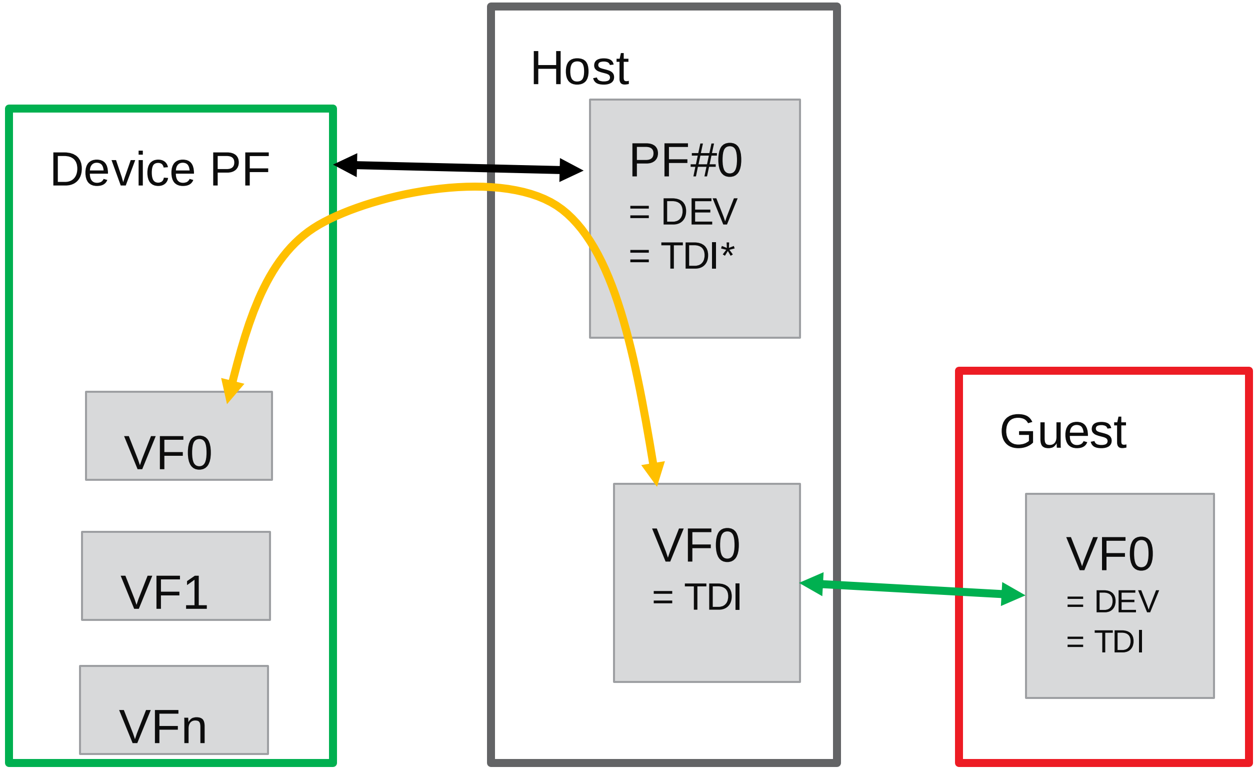
AMD
together we advance_

Configuring IDE/TDISP on AMD SEV SNP



TSM module (coordinating upstream, AMD view)

- Allocates per device data
  - DEV: DOE, SPDM, IDE, measurements, certs
  - TDI: TDISP, report, references DEV
- CMA + IDE
  - HostOS
    - DEV_CONNECT (sysfs)
    - DEV_DISCONNECT (sysfs)
- Pass through (VFIO)
  - HostOS
    - TDI_BIND (KVM) => LOCK, RUN, BIND PREPARE (?)
    - TDI_UNBIND (KVM ioctl)
    - TDI_GUEST_REQUEST (?)
  - GuestOS
    - Guest initiated TDI_LOCK, TDI_RUN (?)
    - TDI_VALIDATE (short for "pvalidate" instruction) (?)
- Common
  - TDI_STATUS (sysfs)
  - Certificates/measurements/report, share sysfs with CMA (?)

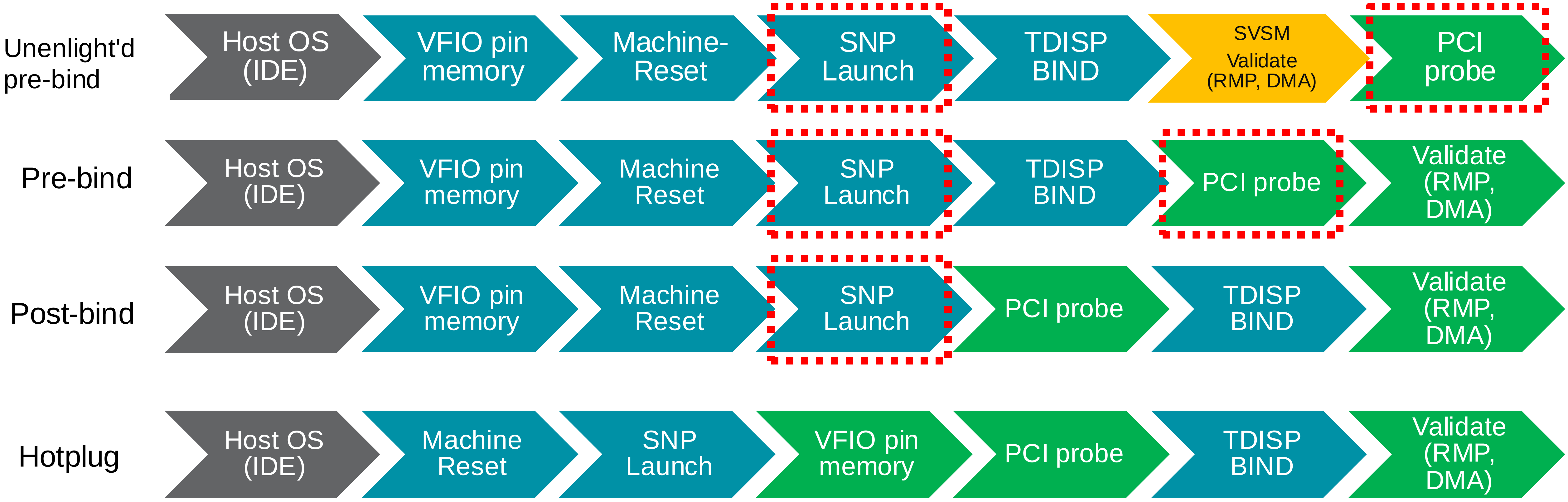


Legend:
(?): "do we need this"
VERB: verbs to implement
TDI*: meaningful only when not SRIOV

TEE: Trusted Execution Environment
TDISP: TEE Device Interface Security Protocol == "Secure VF"
IDE: Integrity and Data Encryption == "Encrypted PCIe link"
CMA: Component Measurement and Authentication == "Authenticated device"
SPDM: Security Protocol and Data Model == "Secure config space access"
DOE: Data Object Exchange == "PCIe config space blob"

AMD
together we advance_

Enlightenment + pre/post/hotplug-bind



Unenlight'd pre-bind	Host OS (IDE)	VFIO pin memory	Machine-Reset	SNP Launch	TDISP BIND	SVSM Validate (RMP, DMA)	PCI probe
Pre-bind	Host OS (IDE)	VFIO pin memory	Machine Reset	SNP Launch	TDISP BIND	PCI probe	Validate (RMP, DMA)
Post-bind	Host OS (IDE)	VFIO pin memory	Machine Reset	SNP Launch	PCI probe	TDISP BIND	Validate (RMP, DMA)
Hotplug	Host OS (IDE)	Machine Reset	SNP Launch	VFIO pin memory	PCI probe	TDISP BIND	Validate (RMP, DMA)

Host/KVM QEMU SVSM GuestOS

IDE == PCIe link encryption
Validate (RMP, DMA) == tell PSP to enable secure MMIO + DMA

Questions:

1) How much of guest enlightenment
2) Sequencing

COPYRIGHT AND DISCLAIMER

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. The information contained herein is subject to change and may be rendered inaccurate releases, for many reasons, including but not limited to product and roadmap changes, component and motherboard version changes, new model and/or product differences between differing manufacturers, software changes, BIOS flashes, firmware upgrades, or the like. Any computer system has risks of security vulnerabilities that cannot be completely prevented or mitigated. AMD assumes no obligation to update or otherwise correct or revise this information. However, AMD reserves the right to revise this information and to make changes from time to time to the content hereof without obligation of AMD to notify any person of such revisions or changes.

THIS INFORMATION IS PROVIDED 'AS IS." AMD MAKES NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE CONTENTS HEREOF AND ASSUMES NO RESPONSIBILITY FOR ANY INACCURACIES, ERRORS, OR OMISSIONS THAT MAY APPEAR IN THIS INFORMATION. AMD SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. IN NO EVENT WILL AMD BE LIABLE TO ANY PERSON FOR ANY RELIANCE, DIRECT, INDIRECT, SPECIAL, OR OTHER CONSEQUENTIAL DAMAGES ARISING FROM THE USE OF ANY INFORMATION CONTAINED HEREIN, EVEN IF AMD IS EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.