presented by AMD

AMD Security and Server innovation

UEFI PlugFest— March 18-22, 2013
Roger Lai
AMD TATS BIOS Development Group
Agenda

• Exciting New Developments at AMD
  – Platform Security Processor
  – Transform Datacenter industry
• BIOS innovation
  – boot speed enhancements
  – Firmware security innovations
• Summary
• Q&A
AMD BRIDGES THE X86 AND ARM® ECOSYSTEMS FOR THE DATA CENTER
The rise of choice

• For the past 20 years, there has been only one choice for industry-standard servers – x86
• Workloads were homogeneous and matched to the x86
• The past 5 years have exploded the one-size-fits-all model
• Workloads have changed, and continue changing at unprecedented rates
• The fastest growing are small and highly parallelized workloads
• ARM® CPU’s are particularly well suited for these workloads
Exploiting efficient processor cores requires a leading-edge fabric

- If each ARM CPU is linked directly to the network, you have efficient computing but inefficient networking.
- Fabrics solve this problem – they link together efficient CPU’s into a cluster, and the cluster is linked to the network.
- SeaMicro’s Input/Output (I/O) Virtualization Technology
- SeaMicro’s TIO™ (Turn It Off) technology
Recent Announcement: AMD will develop 64-bit ARM®-based processors for servers

• Production of ARM technology-based AMD Opteron™ processors for servers in 2014
• ARM technology-based processors will embed the AMD SeaMicro Freedom™ Fabric, the industry’s premier supercompute fabric
• AMD will continue to design x86 CPU’s and APU’s for client and server markets
• Strong Sever expertise in AMD

The AMD Advantage: Differentiation and Choice

CPU  APU  Fabric
AMD offers the right solutions for leading workloads

**Clouds / Mega Data Centers**
- Public & private cloud
- Hosting
- Big Data Analytics
- Hadoop / Cassandra
- Caching / Memcached
- Linux® / Apache / PHP

**Streaming / Mobile**
- Virtual Desktop
- Streaming Media
- Remote Gaming
- Facial Recognition
- Video Encoding
- DRM

**HPC / Simulation**
- Machine Learning
- Commercial CAE
- Oil & Gas Exploration
- Biosciences
- Rendering

**ARM**
- Power efficiency and Open Source ecosystem

**x86**
- Performance and Established Workloads
PLATFORM SECURITY
PROCESSOR
Introduction of PSP

- AMD / ARM strategic security partnership
  - Based on TrustZone architecture
  - Promote hardware, software, and services ecosystem

- AMD Platform Security Processor
  - Licensed ARM Cortex-A5 core with TrustZone
  - Intend to productize across all AMD APUs/CPUs

- Mullins planned to be the first AMD SOC with PSP support
AMD PSP w/ TrustZone technology

- The PSP is an integrated coprocessor next to the AMD64 cores
  - The PSP can run a certified secure OS/kernel
  - The PSP can use Trusted Service Managers for provisioning and lifecycle management
The Platform security processor

- Dedicated security subsystem integrated within APU
- PSP hardware includes:
  - Dedicated 32-bit microcontroller
    - (ARM® with TrustZone technology)
  - Isolated on-chip ROM & SRAM
  - Access to system memory / resources
  - Secure off-chip NV storage
    - Access for firmware and data
  - Cryptographic co-processor (CCP)
    - RSA (1024-, 2048-, and 4096-bit)
    - SHA (SHA1, SHA-224, SHA-256)
    - ECC (basic mathematical computations)
    - AES engine (ECB, CBC, CFB, OFB, CTR, CMAC, XTS-AES128)
    - True Random Number Generator (RNG)
Platform security processor use cases

• Platform Security
  Foundational support
  – Trusted Execution Environment
  – HW Validated Boot
  – Cryptographic acceleration
  – TPM 2.0 functionality

• Client solutions enablement
  – 3rd party solutions – e.g., payments, anti-theft, identity management, data protection, anti-malware, content protection, bring-your-own-device

• End-to-end / client-to-cloud
  – 3rd party solutions – e.g., vertical solutions, policy enforcement, integrity monitoring, audit & asset management, virtual HSM
HARDWARE VALIDATED BOOT
Hardware Validated Boot

- **Hardware Validated Boot** is AMD’s implementation of HW rooted Boot Integrity:
  - An immutable On-Chip ROM in PSP HW forms the Root of Trust
  - PSP authenticates the first block of BIOS code before releasing the x86 processor from reset
  - The BIOS continues the authentication chain
  - This method authenticates the System ROM contents on each boot, not just during updates
  - It can be thought of as moving the root of the UEFI Secure Boot trust chain to PSP HW
POWER MANAGEMENT
SUSPEND/RESUME
S3 Suspend Flow

- SMM Handler trap for S3 command
- Notifies PSP of S3 enter
  - Context of all cores are saved
- Wait for PSP to Ack
- Complete write to PM_CNT register
S3 Resume Flow

- Load and verify PSP off-chip
- Restore S3 save state of CPU cores by PSP
- Transfer control to BIOS and continue S3 resume-path
  - DRAM is ready on X86 resume

Overall complete NEW change in BIOS resume path
BIOS INNOVATION – BOOT SPEED ENHANCEMENTS
Boot Speed Enhancement

• UEFI Legacy-Free booting means no CSM gets loaded. This saves time.
  – (When “Secure Boot” is enabled, no CSM will be loaded.)
• Some systems have SSD hard drives, which also save time.
• Customized customer platform BIOS
• Increase SPI access frequency
• Set SMM Area attribute to WB
• USB Enumeration takes a lot of time
  – UEFI 2.3.1c defines a “boot-options” variable
• AMD PSP
  – AMD PSP CCP HW acceleration for Secure boot
  – Memory is available on x86 resume
BIOS INNOVATION - FIRMWARE SECURITY INNOVATIONS
Why does BIOS need Security?

• **Threats to the System BIOS**
  – Firmware has attracted increasing malware attention
  – BIOS is an attractive target:
    • Persists through power cycles
    • Has full privileges and direct HW access
    • BIOS mostly absent at run time, but…
    • SMM persists, and is very powerful
  – BIOS updates can be initiated during OS runtime, so...
  – Malicious updates could potentially be widely distributed via the web
  – DoS attacks do not need to be very sophisticated
Authenticated BIOS Updates

- BIOS ROM is trusted as it leaves the factory
- BIOS protects the ROM in the field against unauthorized re-flashing
  - BIOS must lock Flash on each boot before running untrusted code
    - Flash ROM is open at reset (to allow updates)
    - Silicon vendor chipsets provide HW methods for locking out Flash updates
- Any BIOS update must be signed by the OEM and authenticated on the platform before the update can proceed

- The goal is to prevent widely distributed web-based attacks on firmware
- NIST Special Publication 800-147 describes Authenticated Updates in detail
UEFI secure boot – Digital Signatures

1. Message
2. Hashing Algorithm
   - Hash Value
3. Signature Algorithm
4. Private Key
5. Signed Message
6. Digital Signature

Message + Digital Signature = Signed Message
UEFI secure boot – Digital Signatures

1. **Message**
   - Input to the system

2. **Hashing Algorithm**
   - Converts the message into a fixed-size hash value
   - Output: Hash Value

3. **Signature Algorithm**
   - Uses a public key to sign the hash value
   - Input: Hash Value, Public Key
   - Output: Signature

4. **Validation Signature**
   - Checks if the signature is valid by comparing it with the signed message
   - Input: Signed Message, Public Key
   - Output: Validation Success/Failure
UEFI secure boot

• On each boot, authenticate code before executing
  – The following must be signed: UEFI OptionROM’s/drivers, UEFI applications, OS boot loader

• Secure Boot does **not** require the System ROM image (i.e. UEFI BIOS, GOP VBIOS) to be signed
  – The System ROM is protected by Authenticated Updating

• After hand-off to the OS loader, the OS can continue the trust chain

• UEFI 2.3.1c, Chapter 27 provides the tools:
  – Certificate formats, data structures, protocols
  – Authenticated variables for:
    • KEK, *signature database* (db), *revoked signatures database* (dbx)
BIOS Security – Current industry Progress

• “Authenticated BIOS Updates” and “UEFI Secure Boot” are included on many new systems, because they are required for a Windows 8 client logo

• The UEFI Forum is also working with the Linux community to make the benefits of Secure Boot available to Linux users
  – Some Linux® distributions have already added this support
  – These protections are available to all OS’s that wish to use them
Summary

• Cloud changes everything
  – Only AMD can deliver 64-bit ARM\textsuperscript{®}-based server processors
  – Only AMD can deliver low power and better performance to datacenter.
  – AMD is poised to be a disruptive force in servers

• BIOS Security needs to improve
  – UEFI and AMD PSP security architecture can address needs
  – Follow AMD PSP practices on implementing hardware and firmware
  – Firmware is becoming more secure
  – Much of this innovation is due to the collaborative efforts of the UEFI Forum
Resources and links

• AMD and ARM® 64 Announcement and Introduction Event

• AMD PSP Details at: AMD Fusion Developer Summit - Digital
  – After logging in below, click on the Security track, and then either the PDF or the video of “A Unified Security Ecosystem”
  – [https://vts.inxpo.com/Launch/Event.htm?ShowKey=8934%0A](https://vts.inxpo.com/Launch/Event.htm?ShowKey=8934%0A)

• The UEFI Forum (for data and/or membership):

• NIST Special Publication 800-147 (on Authenticated BIOS Updates):
Acronym decoder

- APU - Accelerated Processing Unit (fusion of CPU and GPU on one die)
- BYOD – Bring Your Own Device (to work)
- CSM – Compatibility Support Module (legacy BIOS services layered on top of UEFI BIOS)
- DoS – Denial of Service (malware attack technique)
- GOP – Graphics Output Protocol (UEFI Video BIOS; replaces VGA)
- GUID – Globally Unique IDentifier (128-bit naming scheme with very low chance of collisions)
- HII – Human Interface Infrastructure (allows IHV’s to extend UEFI BIOS Setup)
- HSM – Hardware Security Module (secure cryptographic co-processor)
- ISA – Instruction Set Architecture (a processor’s programming model (op-codes, registers, etc.))
- IHV / ISV – Independent Hardware Vendor / Independent Software Vendor
- NIST – National Institute of Standards and Technology (US Government standards body)
- PSP – Platform Security Processor (AMD’s upcoming security co-processor)
- RTM - Root of trust for measurement
- SMM – System Management Mode (x86 HW method for executing firmware during OS runtime)
- SOC – System On a Chip (Integrated Circuit with multiple major functions on one chip)
- TCG – Trusted Computing Group (security standards body)
- TEE - Trusted Execution Environment (TrustZone is one example)
- TPM – Trusted Platform Module (hardware-based security chip with TCG-specified functions)
- UEFI – Unified Extensible Firmware Interface (new firmware interface for booting an OS)
Q&A
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 for many reasons, including but not limited to product and roadmap changes, component and motherboard version changes, new model and/or product releases, product differences between differing manufacturers, software changes, BIOS flashes, firmware upgrades, or the like. There is no obligation to update or otherwise correct or revise this information. However, we reserve the right to revise this information and to make changes from time to time to the content hereof without obligation to notify any person of such revisions or changes.

NO REPRESENTATIONS OR WARRANTIES ARE MADE WITH RESPECT TO THE CONTENTS HEREOF AND NO RESPONSIBILITY IS ASSUMED FOR ANY INACCURACIES, ERRORS OR OMISSIONS THAT MAY APPEAR IN THIS INFORMATION.

ALL IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT WILL ANY LIABILITY TO ANY PERSON BE INCURRED FOR ANY DIRECT, INDIRECT, SPECIAL OR OTHER CONSEQUENTIAL DAMAGES ARISING FROM THE USE OF ANY INFORMATION CONTAINED HEREIN, EVEN IF EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Trademark Attribution

AMD, the AMD Arrow logo and combinations thereof are trademarks of Advanced Micro Devices, Inc. in the United States and/or other jurisdictions. Other names used in this presentation are for identification purposes only and may be trademarks of their respective owners.

©2012 Advanced Micro Devices, Inc. All rights reserved.
Thanks for attending the UEFI Spring PlugFest 2013

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

presented by