AMD's robust silicon-level security features are competitive, consistent, and comprehensive. One of AMD's strengths is that security and virtualization technologies are designed into every AMD processor, including our AMD Opteron™ 6000 and 4000 Series processors. Regardless of the unit chosen, customers buying AMD have full access to these features.

**Processor Virtualization**
Silicon-level virtualization technology allows abstraction of physical system hardware from machine image through the hypervisor, thereby creating a firewall between attackers and physical storage.

**I/O Virtualization**
Protects memory from peripheral-based attacks, by enabling guest VMs to directly and securely use peripheral devices, such as Ethernet, accelerated graphics cards, and hard-drive controllers.

**Advanced Encryption Standard (AES) Instructions**
Provides hardware acceleration to enable fast and secure data encryption and decryption.

All are important in virtualized environments and in the context of cloud computing.

Since 2006, all 65 nm AMD processors except AMD Sempron™ have AMD Virtualization (AMD-V™) technology. Since 2008, all 45 nm AMD processors have AMD-V.

Since 2009, certain AMD chipsets have I/O virtualization. AMD products beginning with those based on the “Bulldozer” CPU core, including the “Zambezi” desktop processor and the “Interlagos” server processor, have AES instructions.

**Secure Boot/System Initialization**
Verifies status of multiple processes and components before initializing bios and OS kernel.

Helps prevent attacks associated with firmware/software that may be out-of-date and includes known vulnerabilities, or it helps prevent attacks where there has been malicious modification to good software (e.g., someone adds malware to the boot image of Windows).

- Since 2006, AMD has incorporated a silicon-level feature called SKINIT in all CPU products to support secure boot.
- Before taking the next step to complete a “secure boot” solution with BIOS and OS integration, AMD is monitoring the market for indication that this is a real need.

If and when the market sets a clear direction on this security feature, AMD is ready to work with ecosystem partners to bring a full solution to market. SKINIT does require a TPM module to enable full functionality, which will add cost.
### Securing the Platform / CPU and Chipset

<table>
<thead>
<tr>
<th>Feature</th>
<th>AMD</th>
<th>Intel</th>
</tr>
</thead>
</table>
| **NX Bit (No eXecute)** – technology used by CPUs to segregate areas of memory. Working in concert with OS can be used to prevent certain types of malware from executing harmful code. | EVP (Enhanced Virus Protection) – available on all 64-bit AMD CPUs (starting in 2003) | XD Bit (Execute Disable Bit) – available with Pentium 4 “Prescott” core (starting in 2004)
| **Secure Boot/Secure Kernel Initialization** – hardware extensions that provide a higher level of trust and control over computer systems. | SKINIT Instruction – introduced in AMD CPUs in 2006 | Trusted Execution Technology (TXT) – not all Intel processors support TXT
| **Hardware-assisted Virtualization** – technology that creates isolation between Virtual Machine partitions. | AMD-V™ – introduced in AMD processors in 2006 | VT-x – introduced by Intel in 2005; not available in all Intel processors
| **I/O Virtualization** – enables guest VMs to directly and securely use peripheral devices, such as Ethernet, accelerated graphics cards, and hard-drive controllers. | IOMMU – available in certain AMD chipsets starting in 2009 IOMMU v2 supported in “Trinity” | VT-d – available in certain Intel chipsets starting in 2008
| **AES Instructions** – provides hardware acceleration to enable fast and secure data encryption and decryption using the Advanced Encryption Standard (AES). | Called AES Instructions Supported in “Bulldozer” core (“Zambezi,” “Interlagos,” “Trinity”) | Called AES-NI (AES New Instructions) Intel® Xeon® 5600 series Intel® Core™ i5 600 series

### Securing the Platform / Other SW/HW Components

<table>
<thead>
<tr>
<th>Feature</th>
<th>AMD</th>
<th>Intel</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Trusted Platform Module (TPM)</strong> – TPM is a secure cryptoprocessor that can store cryptographic keys that protect information.</td>
<td>Selected platforms</td>
<td>Selected platforms</td>
</tr>
<tr>
<td><strong>Software-based Disk Encryption</strong> – prevents unauthorized access to data storage. “Full disk encryption” is used to signify that everything on a disk is encrypted, including the programs that can encrypt bootable OS partitions.</td>
<td>Various software available (for example, Windows Bit Locker)</td>
<td>Various software available (for example, Windows Bit Locker)</td>
</tr>
<tr>
<td><strong>Hardware-based Disk Encryption</strong> – prevents unauthorized access to data storage. Hardware-based “full disk” encryption systems that can encrypt the entire boot disk, including the master boot record (MBR).</td>
<td>Selected platforms</td>
<td>Selected platforms</td>
</tr>
</tbody>
</table>
| **Anti-Theft (AT) Technology** – if laptop is lost or stolen it can be rendered inoperable by blocking the boot. | AT software technology available from ISVs and open source software | Hardware-based AT technology is available in selected 2nd generation Intel Core and 2nd generation Intel Core vPro™ processors. Must be activated with a service subscription from an Intel AT-enabled service. Intel AT adds incremental hardware-based enhancements to features already available through anti-theft SW vendors.

---


©2012 Advanced Micro Devices, Inc. All rights reserved. AMD, the AMD Arrow logo, AMD Opteron, AMD Sempron, AMD Virtualization, AMD-V, and combinations thereof are trademarks of Advanced Micro Devices, Inc. Other names are for informational purposes only and may be trademarks of their respective owners. 51526A

*Table continued on next page*