Secure Hardware and the Creation of an Open Trusted Ecosystem

Dr. Leendert van Doorn
AMD
Today’s Security Challenges

- **Mobility (seamless client to cloud)**
  More devices and data per person, centralized data repositories, subsidized platforms, controlled user experience, metering /licensing, consumer data protection

- **Consumerization of IT (BYOD)**
  Personally owned devices employed in enterprise environments, protection of corporate information, address regulation and compliance requirements

“A recent survey completed by Gartner indicates that CIOs fully expect to support up to three mobile operating systems by 2012 and that 20% of devices will be employee-owned by that year."

Today’s Security Challenges (cont’d)

- **Cloud computing (separation & transparency)**
  Multi-tenancy and lack of control, with Governance, Risk & Compliance driving separation technologies and the need for transparency and accountability in the cloud to support mission

- **Advanced Persistent Threats (APTs)**
  Advanced and normally clandestine means to gain continual, persistent intelligence on an individual, or group of individuals such as a foreign nation state government

  - Operation Aurora on Google (Jan 2010)
  - Stuxnet worm targeting Iranian nuclear sites
  - Night Dragon targeting energy companies
  - Flame targeting PCs in the Middle East

The Trusted Computing Conference
Security starts at the root of a system
- Anything short of that allows an attacker to interpose the bootstrap process and enables BIOS viruses and other Advanced Persistent Threats (APTs).

Security needs to be anchored within the hardware so that it cannot be circumvented

Security needs to be an active and dynamic component of the system
- Security functions change over time or per customer segment (e.g. consumer, commercial or Cloud servers).
- You should be able to add security functions to your platform at manufacturing time, install time or even later.
The Security Ecosystem Today Is Fragmented

- It is difficult for a security ISVs to anchor their solutions in hardware

- Partial solutions exists for different operating systems but depend on many complex layers

- The hardware ecosystem is very fragmented with many proprietary solutions

- These proprietary solutions rarely allow ISV extensions

- We need a more flexible solution …
What Is AMD Doing About This?

- In 2012 AMD partnered with ARM
  - AMD added an ARM embedded microcontroller with ARM TrustZone® technology to some of its product roadmap as a security foundation

- This is designed to provide a consistent security foundation is beneficial for whole-system security and end-to-end protection across heterogeneous environments
  - Share goal of promoting hardware, software, and services ecosystem based on ARM TrustZone® technology
  - TrustZone® is a well proven industry security technology

- What does this mean for the industry?
  - AMD and ARM together provide scale and breadth of products
  - Broad ecosystem based on adoption of TrustZone® technology and open industry-standards across all types of computing platforms
TrustZone® technology provides a Trusted Execution Environment (TEE)

- Protects the secure world from software attacks from the normal world
- Proven security technology in mobile, tablet and embedded markets
The Trustzone® Ecosystem

- The TrustZone® ecosystem is based on open industry standards such as GlobalPlatform
  - Standard APIs to security services, certification programs, and protection profiles.
  - Proven secure isolation kernels exist such as those produced by Trustonic

- Enables ISVs to develop secure applications and be portable across a wide range of solutions

- AMD’s security technology maintains portability, even at the application binary interface (ABI) level, for trusted applications

- Different security solutions for alternate segments
  - E.g., Consumer: mobile payments, password vaults, anti-malware, content protection
  - E.g., Commercial: asset protection, document control, bring-your-own-device protection
The PSP is an integrated coprocessor next to the AMD64 cores

- The PSP runs a certified secure OS/kernel
- The PSP can use Trusted Service Managers for provisioning and lifecycle management
The Platform Security Coprocessor (Hardware)

- 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
  - 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)
  - Zlib (compression and decompression)
  - TRNG
AMD’s Security Roadmap

**2012**
- Core Security
  - Trusted Platform Module and Secure Kernel Initialization
  - Virtualization extensions and 2° gen. I/O Virtualization
  - AES Instructions

**2013**
- Secure Platform Enablement
  - Platform Security Processor with fixed security functions (introduction)
  - Cryptography acceleration for AES, RSA, ECC, SHA, TRNG
  - Secure boot capabilities

**2014**
- Secure Platform Deployment
  - Platform Security Processor enabled on all 2014 APUs
  - TrustZone® ecosystem enablement
  - Identity protection, anti-theft, etc. in hardware
Platform Security Processor Use Cases

- **Platform Security Foundational support**
  - Trusted Execution Environment
  - Secure boot
  - Cryptographic acceleration
  - TPM 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
Last week we announced a partnership with Trustonic

- AMD has licensed the Trustonic TEE as its security kernel in the PSP

Trustonic is the industry leader in TEE development

- New company but with years of experience from ARM Secure Services Division, Giesecke & Devrient (G+D) and Trusted Logic Mobility (TLM) TrustZone®
- Industry proven and certified TEE solutions

This underscores AMD’s commitment to developing an open secure ecosystem

- AMD now has access to Trustonic’s extensive partner ecosystem
- Working together on expanding these technologies into the Tablet, PC, Desktop and Server domains.
Summary

- AMD is adding an integrated Platform Security coProcessor (PSP) to its roadmap
  - The PSP is embedded in the SOC
  - The PSP provides a trusted execution environment for AMD and 3rd party security solutions

- AMD is adopting proven technology for its security solution
  - ARM microcontroller with TrustZone® architecture is the foundation for the PSP
  - Using open industry standards

- AMD and ARM are working together in driving and expanding the ecosystem based on TrustZone® technology
  - We have the scale and breadth of products
  - Actively engaged with the security ISVs

- Join us in driving an open industry-standard TrustZone ecosystem
  - Take advantage of new levels of security innovation that were not possible before
Thank You
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.

AMD, the AMD arrow logo, and combinations thereof are trademarks of Advanced Micro Devices, Inc. TrustZone is a trademark of ARM, Ltd. All other names used in this presentation are for informational purposes only and may be trademarks of their respective owners.

© 2013 Advanced Micro Devices, Inc.
Sample text slide with Alis is dolorro conem. Ducium vendaectur solum quo mil ea quias est, sini totas es venis ditat.

Tempero voluptiunte dolestiur reius nonsed quunt officias aut offic te nulpa dolum am entia neculpa as velignam nobiti dignis moluptat erferitae venitis sim dit aut endit landae es aut im rae est ipsaerum que vero est, offictus voloribus, officipsunt occae. Namus verio. Soloribus sus a hillam et esercid
Disclaimer
Sample Bulleted Slide

Multiple Lines of Text

• First level bullet
  – Second level bullet
    » Third level bullet
<table>
<thead>
<tr>
<th>Row</th>
<th>Column 1</th>
<th>Column 2</th>
<th>Column 3</th>
<th>Column 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Row 1</td>
<td>Cell Data</td>
<td>Cell Data</td>
<td>Cell Data</td>
<td>Cell Data</td>
</tr>
<tr>
<td>Row 2</td>
<td>Cell Data</td>
<td>Cell Data</td>
<td>Cell Data</td>
<td>Cell Data</td>
</tr>
<tr>
<td>Row 3</td>
<td>Cell Data</td>
<td>Cell Data</td>
<td>Cell Data</td>
<td>Cell Data</td>
</tr>
<tr>
<td>Row 4</td>
<td>Cell Data</td>
<td>Cell Data</td>
<td>Cell Data</td>
<td>Cell Data</td>
</tr>
<tr>
<td>Row 5</td>
<td>Cell Data</td>
<td>Cell Data</td>
<td>Cell Data</td>
<td>Cell Data</td>
</tr>
<tr>
<td>Row 6</td>
<td>Cell Data</td>
<td>Cell Data</td>
<td>Cell Data</td>
<td>Cell Data</td>
</tr>
</tbody>
</table>