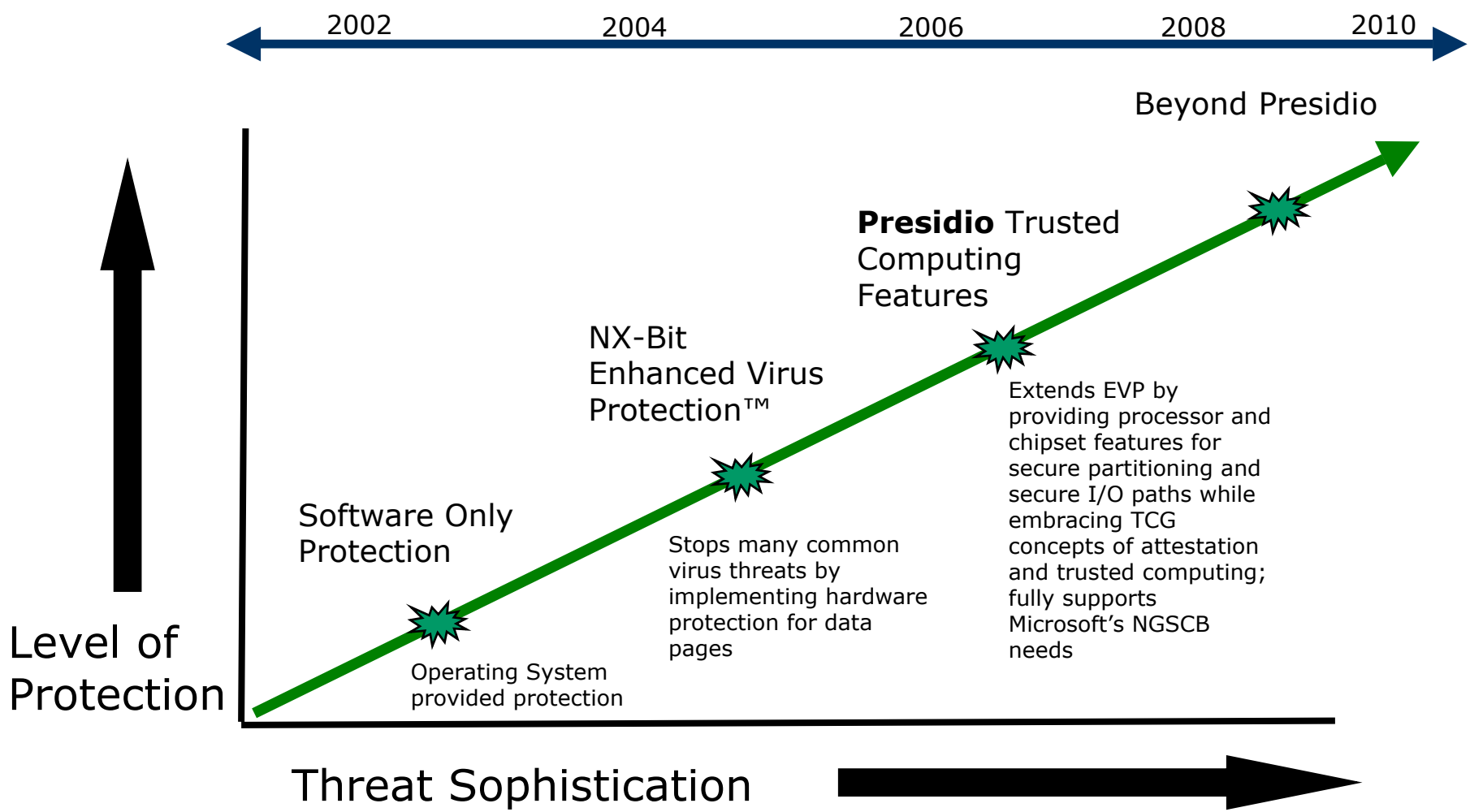
AMD's Vision for Trustworthy Computing

Geoffrey Strongin

Platform Security Architect

AMD

AMD's Security Vision



Meeting The Challenge – Building Trustworthy Platforms

- Addressing the problems of Privacy, Security and Third Party Trust requires changing the PC platform
- Changes to both hardware and the OS are needed
- AMD is working with key partners and the entire industry in a broad-based effort to increase the trustworthiness of the PC platform
  - The key standards group in this area is the Trusted Computing Group
  - AMD is a Founder and Promoter of the Trusted Computing Group
  - AMD sees the TCG as the BEST way for the computing industry to address the collective need for increased trust in computers
- AMD believes that the computer industry has a shared responsibility to improve computer security
  - Open standards are essential to the success of this effort

Meeting the Challenge – The role of TCG

- The Trusted Computing Group has critical mass
  - More than 80 corporations are TCG Members
- TCG has the "architectural vision" for Trusted Computing
  - Core TCG Technology:
    - Determining Platform State (in spite of attacks)
    - Reporting this Platform State (in spite of attacks)
    - Protecting data against unauthorized disclosure
    - Protecting user privacy
  - Experts from leading technology companies working cooperatively
- TCG has the correct charter and mission
  - Vendor neutral
  - Cross Platform (PC's, Servers, phones, PDA's, peripherals etc.)
  - Open specifications for "building blocks"
  - Open membership
  - RAND IP model

Role of TCG cont.

- TCG also has the right internal structure
  - Open Workgroup Formation Process
    - Allows TCG to be "member driven"
- TCG is also at the forefront of Government interactions on Trusted Computing
  - EU
  - German Federal Ministries
    - Economics and Labor
    - Internal Affairs
  - CISTC
- TCG is also at the forefront in defining and advocating proper usage of Trusted Computing Technology
  - TCG Best Practices Principles

Specific AMD Goals

- Raise the bar for PCs by addressing the trust related issues
- Minimize the system cost impact
- Preserve the billions of dollars in investment made by IHVs and ISVs
- Provide strong privacy protections while increasing security
- Enable new uses for the PC and new revenue streams for OEMs

AMD Platform Architecture Changes
Scope:

- New Hardware Capabilities
  - Isolated Execution Space (CPU Feature)
  - Enhanced Virus Protection (CPU Feature)
  - Storage Sealing (TPM Feature)
  - Secure Initialization (CPU/Chipset/TPM Feature)
  - Secure Input (Chipset/CPU Feature)
  - Secure Output (Chipset/CPU Feature/GPU Feature)
  - Remote Attestation (Chipset/CPU/TPM Feature)