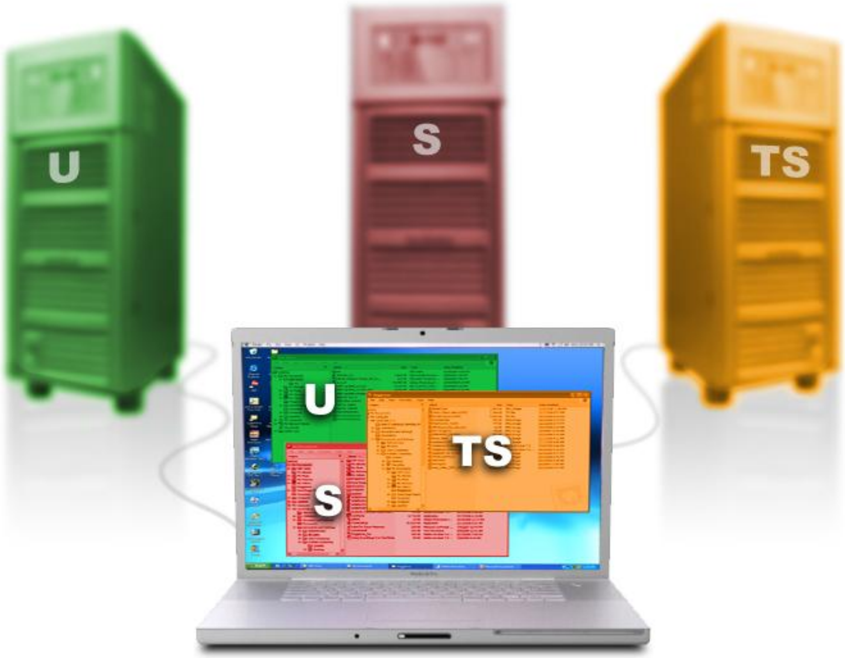
High Assurance Platform (HAP)
High Assurance Challenges

Rob Dobry
Trusted Computing
NSA Commercial Solutions Center
04 & 05 August 2009

What is HAP?

HAP is being developed to provide users with two primary capabilities:

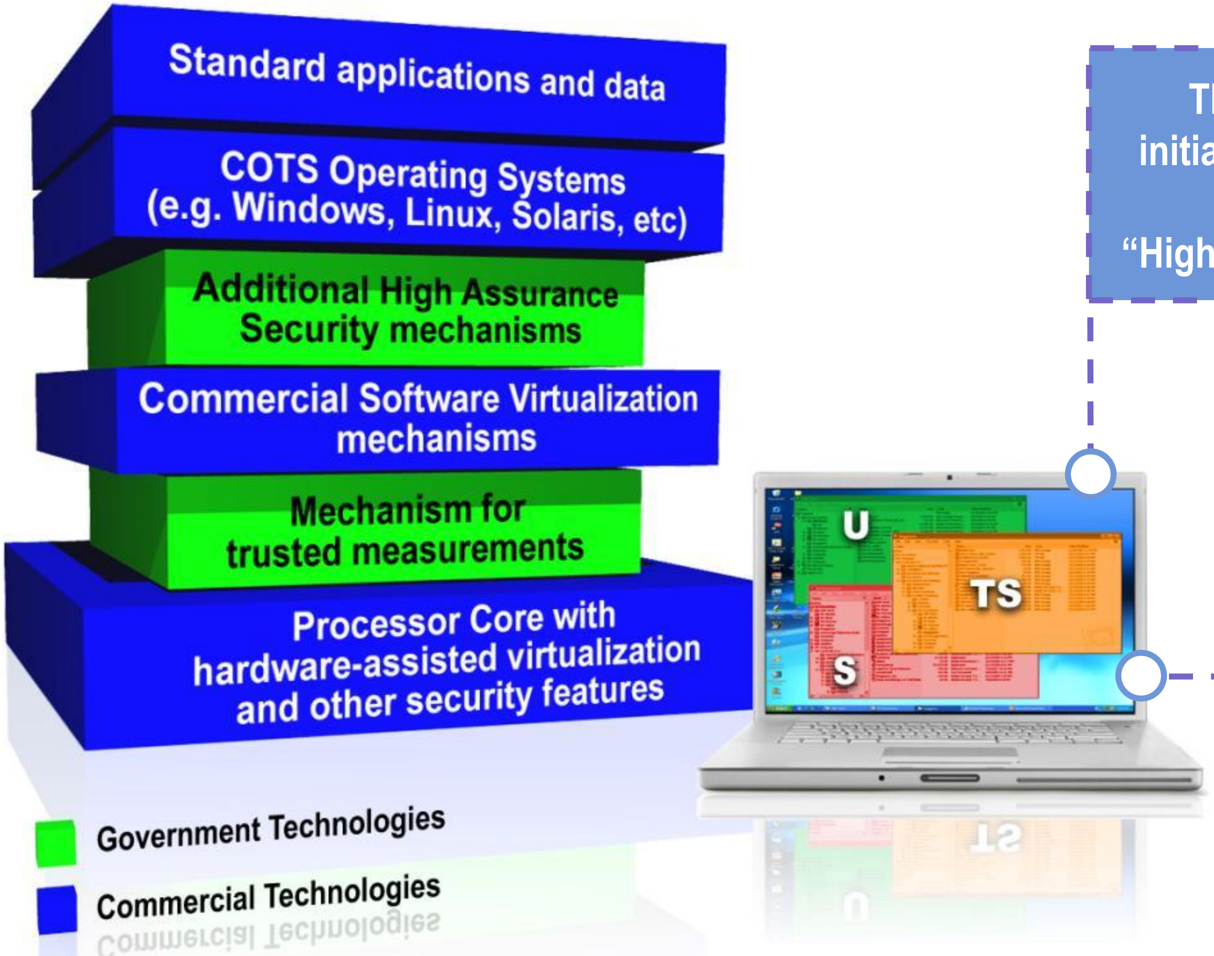
1. Provide secure access to multiple domains or networks from a single workstation
2. Allow secure data movement between domains



Program Goals

- Deliver a computing platform architecture and roadmap leading to U→TS on the same platform
- Allow secure data movement between domains
- Deliver certified and accredited reference implementations that can be built, modified, and commercialized by industry
- Run legacy applications and systems
- Be enclave agile / remotely reconfigurable
- Support common peripherals
- Incrementally deliver near-term, meaningful capabilities
- Leverage COTS HW & SW to the maximum extent possible
- Develop government components only when absolutely necessary to achieve very specific results

Fusion of Commercial Relevant Technologies and High Assurance


Standard applications and data
COTS Operating Systems
(e.g. Windows, Linux, Solaris, etc)
Additional High Assurance Security mechanisms
Commercial Software Virtualization mechanisms
Mechanism for trusted measurements
Processor Core with hardware-assisted virtualization and other security features
🟩 Government Technologies
🟦 Commercial Technologies
U
TS
S

The fusion of commercial initiatives plus trusted software create a "High Assurance Platform" (HAP)

A HAP can support both trusted separation of domains and multi-level Cross-Domain

What Have We Delivered?

- Release 1
  - Capabilities
    - Single Level Separation
    - Measured Launch/Platform Attestation/Passive NAC
  - Certification & Accreditation Status:
    - SABI: ST&E completed
    - TSABI: Completed – waiting for the ATO from ODNI
  - HAP R1 Workstation commercially available through Dell NOW

What Are We Building?

- Release 2
  - Capabilities
    - Single Level Separation between TS/S or S/U
    - Runtime Measurements/Restrictive NAC/vTPM
  - Will run on same hardware baseline as Release 1
  - Include laptop and tactical server instantiation

Where we are headed (R3 Capabilities)

- Separation
- Sharing
- Security
- Manageability

Separation

- 2-Domain Separation
  - Unclassified thru Top Secret
- Device Driver Isolation
  - Hardware enforced
- Direct Device Assignment
  - Assign specific ports/devices to specific computing environments

Sharing

- Single sign-on
- Multi-factor Authentication / Multi-level token
  - Authenticate across security domains
- Cross domain sharing
- Cross domain discovery
- Cross domain collaboration
- Create Communities of Interest (COI)
- Trusted service interface
  - Other computing environments leverage HAP security properties
- General user access
  - User at lowest security level can use platform (PL5)

Security

- Mutual Attestation
  - Machine / Machine
  - Machine / Network enterprise
- Phased integrity measurements
  - Freshness of measurements
- Integrity based policy enforcement
  - Evaluate measurements
- Data at rest protection
- Zeroization
- Trusted path / Trusted display
  - Protect data paths / displays
- Network event analysis

Manageability

- Single wire
- Remote administration
- Just enough Operating System (JeOS)
- Interoperability
- On demand secure launch
  - Non-secure to secure and back
- Form factor
  - Desktop
  - Laptop
  - Server
  - Embedded

Areas of Challenge: Release 3

- Bare Metal Hypervisor
  - Tailored for enterprise server/client
- Virtualization
  - Decomposition of Host OS into a virtual trusted platform
  - Server-side sharing for low-to-high movement of data
  - Server-side sharing for high-to-low movement of data
  - Secure Virtual Appliance for Single NIC
- Attestation
  - Measurement of mobile VMs
  - Measurement of hypervisor and virtual trusted platform
  - Integration of measurements across domains
  - Late launch just-in time client
- Administration
  - Large scale VM configuration management
  - Automated provisioning for VM-based COI
  - Coordinated provisioning between client and server for COI
- I&A
  - Single sign on
- Audit
  - Integrated audit of virtual trusted platform and guest VMs
- Access Control

  Type enforcing hypervisor

More information

Further questions contact:

Rob Dobry
(410)854-4179
rwdobry@missi.ncsc.mil

Neil Kittleson
(410) 854-4174
ndkittl@nsa.gov

Capability Roadmap

	Release 1	Release 2	Release 3 Concepts
Release Availability	Q4 FY08	Q1 FY10	Q4 FY12
Certification	SABI/TSABI	UCDMO	UCDMO
Platform Integrity	Measured Launch Platform Attestation Passive NAC	Runtime Measurement Collection Platform Attestation Restrictive NAC Incorporation of virtual TPMs (support guest integrity collection/reporting)	Increased granularity of Attestation measurements, including: Additional boot-time measurements, Measurement of complete Guest and Helper VMs and Virtual Appliances, Dynamic Guest VM measurement services for COI attestation use
Enterprise Management	Local Administration Manual Provisioning/ Installation Manual Key Management	Enterprise Administration Remote Provisioning/Installation Automated Key Management Enterprise Software Distribution	Customizable User Role functionality Improved Admin and User graphical interfaces Increased ESS-to-Local (legacy) network integration
Network Infrastructure Reduction	One wire per security domain	Integration of VPN tunneling solution enables wire/nic to be shared	Single NIC configuration via approved Data-in-Transit solution
Deployment Models	Untethered/Tethered	Untethered/Tethered/Peer-to-Peer	Untethered/Tethered/Peer-to-Peer
Information Sharing	None	Support virtualized guard/filter to process cross domain transfers. Instantiate, deploy, and execute secure collaboration environments (COIs).	Platform supported cross domain capabilities Cross Domain Collaboration Infrastructure support Low-to-High Cut and Paste
Advanced Security Controls	Mandatory Access Control Discretionary Access Control Role Based Access Control	Data-at-Rest Encryption Policy Enhancements Launch Control Policy	Trusted Path, Device Driver Isolation, Multi-Factor Authentication, Protection and Encryption of Platform Security Function data, Data-at-Rest Protection for Guest and Helper VMs
Accessbile Virtual Machines	3	4–6	15–20
Form Factor	Workstation	Workstation, Laptop, Tactical Server	Workstation, Laptop, Server

080704_007v2.ai