

HIGH ASSURANCE PLATFORM[®] (HAP)

Using Trusted Computing Technologies to Provide Security in a Connected World

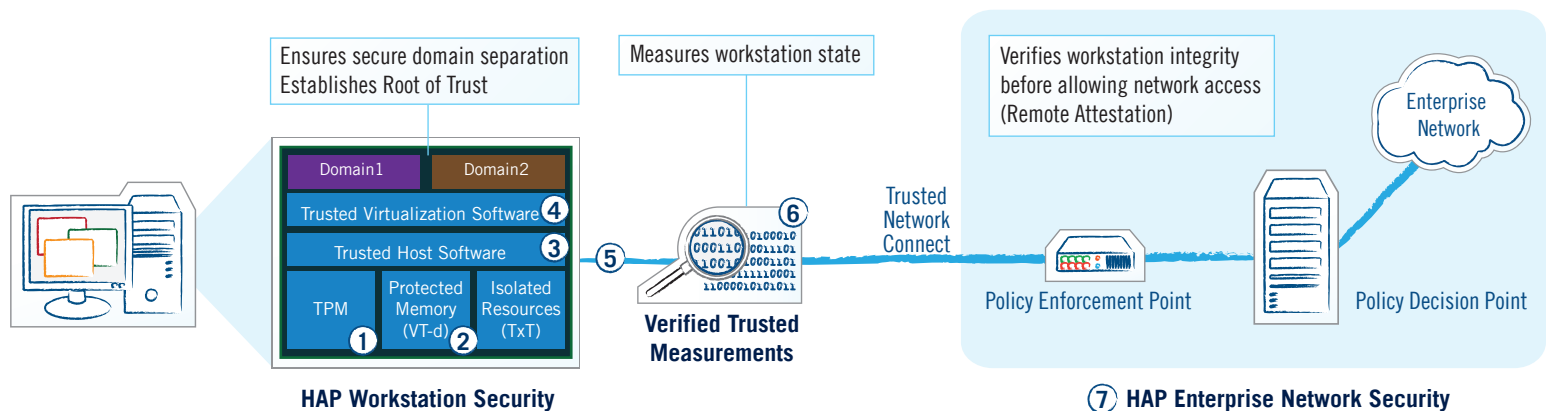


The High Assurance Platform[®] (HAP) Program is an NSA initiative to define a framework for the development of the "next generation" of secure computing platforms. HAP uses commercial Trusted Computing technologies to dramatically improve protection for data, applications, and networks – providing security in a connected world.

Trusted Computing technologies are a set of specifications, products, tools and techniques designed to provide mechanisms, both hardware and software, that ensure that a system is operating in a manner that is expected and for which it was designed (e.g., only authorized software is allowed to run on systems and networks).

Today, a variety of commercial products make limited use of Trusted Computing technologies, but few secure, integrated environments exist. The HAP Program has pioneered the integration of a comprehensive set of commercial Trusted Computing technologies to create reference implementations of secure environments. These reference implementations use hardware and software technologies to dramatically improve workstation and network security.

How Trusted Computing Technologies Are Used in HAP Environments Today



Trusted Platform Module (TPM)

Embedded security chip that secures keys and data. HAP uses the TPM to attest to the machine's identity and the integrity of the software running on it.



Embedded Hardware Virtualization Security

Intel's VT-d and TxT hardware technologies protect execution space and memory, and directly pair I/O devices with domains. HAP uses these technologies to protect resources in one domain from unauthorized access by hardware or software in another domain.



Trusted Operating System

A rigorously tested operating system that is measured and granted privileges to access critical security data and resources. HAP uses a trusted operating system as a host operating system for the secure virtualization software and to tightly restrict the ability of one process to compromise the security of another process.



Secure Virtualization Software

A specially tested commercial hypervisor manages concurrent operation of multiple guest operating systems. HAP uses enhanced secure virtualization software to ensure secure domain separation.



Trusted Boot

The trusted boot process measures the software that is running on a machine each time it boots. HAP securely reports or "attests to" those measurements when required.



Remote Attestation

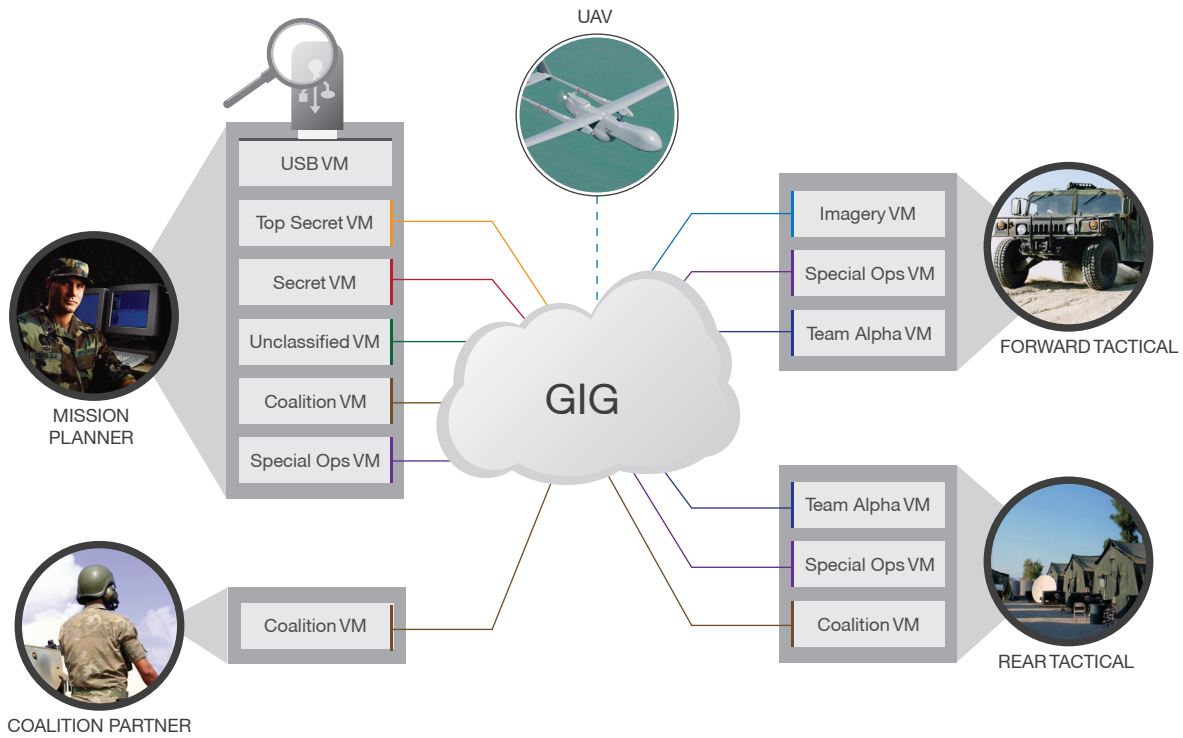
Remote attestation provides "verification" of software state on a client and verifies that proof on a remote machine. HAP uses remote attestation to manage network access control and ensure that only trusted machines in the proper state are allowed on HAP-protected networks.



Trusted Network Access Control

Manages which devices are allowed to access network resources. Trusted network access control utilizes a cryptographic proof or "attestation" that the software on the client is trusted. HAP includes two remote components, a Policy Decision Point (PDP) and Policy Enforcement Point (PEP), to securely manage the validation of the client attestation and control access to the network.

HAP Framework: Benefits for Government



Machine Consolidation

Desktop and server machine consolidation, with full support for U – S and S – TS secure domain separation.

Coalition Collaboration

Secure collaborative workspaces are provisioned in real time with no incremental infrastructure.

Safe Use of Untrusted Devices

Device driver isolation improves I/O security with untrusted devices. Avoids complicated exception process.

Incident Detection & Response

Enhanced administrative controls support real-time incident detection and response.

Mobile Device Support

Secure access to multiple domains can be granted from anywhere.

Secure Disposal

IT organizations can securely erase all data from the hard disk when decommissioning or reassigning machines by destroying the encryption key.



SWaP reduction through multi-domain desktop and server consolidation



Endpoint security via attestation and trusted boot



Low-cost, rapid deployment of secure domains for coalition collaboration



Secure multi-domain support on laptop form factor

HAP R2: Coming Fall 2010

The second reference implementation of HAP, to be released in the fall of 2010, includes several enhancements:

Client Enhancements

- Laptop form factor support
- Upgrade to RedHat Enterprise Linux 5 with SE improvements
- Expanded TPM use for key storage and generation
- Separate Router & VPN VM
- vTPM for guests
- DMA isolation using Intel® VT-d
- DRTM Launch Control Policy
- Upgrade to VMware WS7
- Single NIC configuration
- 64-bit guest OS support

Enterprise Enhancements

- Open Interface Strategy
- Flexible VM Management
- ESS Certificate Support



Request a HAP Developer Kit

The HAP Program Management Office is making HAP source code and documentation available at no cost to qualified organizations. To become a Partner and receive a Developer Kit for your organization, email the NSA at hap@nsa.gov

For more information, visit www.nsa.gov/hap