YOU CAN'T

Unless you've got HAP

Start building a trusted environment now...

(before it's too late)

IT Decision Makers

HAP reference implementations and commercial solutions are available now in the HAP Developer Kit. With a free Developer Kit you can begin piloting HAP at your agency or company and start building a safer environment.

Technology Vendors

HAP is the foundation for a new, radically safer computing environment. HAP opens a green field of opportunity for vendors to develop component technologies, enhance existing products and offer services that leverage and extend HAP standards.

Request a HAP Developer Kit

The HAP Program Management Office (PMO) is making HAP source code and documentation available at no cost to qualified organizations. To request a HAP Developer Kit for your agency or company, email the HAP PMO at hap@nsa.gov.

HIGH ASSURANCE PLATFORM®

Security in a Connected World

www.nsa.gov/hap hap@nsa.gov 410.854.4463

What makes you think you can trust your computer?

50%

of U.S. computers are now infected - up 66% since 2008

250,000

Attacks per year on DoD Information Systems

85%

of businesses report at least one serious data breach each year

$117,000,000,000

Annual cost of U.S. computer crime

HIGH ASSURANCE PLATFORM®

Security in a Connected World

Establishing Trust

Establishing trust used to be a lot easier. A handshake. A nod. A simple assurance from someone you know. But knowing who to trust in today's networked computing environment is a lot more challenging. Both government and industry have tried to keep up, but we're losing ground. Threats multiply even as our dependence on the network increases. Today's cybersecurity challenges require more than incremental enhancements to existing solutions. What's needed is nothing short of a revolutionary new foundation for secure computing.

Transforming the Computing Environment

The High Assurance Platform ® (HAP) program is a multi-year NSA effort to define a framework for the development of the "next generation" of secure computing platforms. The program couples emerging commercial-off-the-shelf security technologies with a variety of assurance techniques to establish standards that enable a transformation of the computing environment—a new approach to security that reliably protects information, network and applications.

A New Paradigm for Cybersecurity

Unlike conventional cybersecurity solutions that assume devices are safe unless known threats are detected, HAP defines a new security paradigm that assumes devices cannot be trusted until hardware-based integrity measurement is used to confirm their safety.

Key Capabilities of the High Assurance Platform® Environment

Embedded Security Module

The fundamental core of trust in any HAP device - be it a desktop, laptop, server or other device - is the Embedded Security Module (ESM). The ESM provides hardware-based protection of cryptographic keys, stores measurements of device state and helps to prove to a third party that the device is trustworthy.

Device Hardware Security

The internal hardware in a HAP device is built from the ground up to strengthen the security of the computing environment. The HAP hardware memory partition provides a secure connection to the ESM to guard against unauthorized access and separation of resources to isolate different security domains.

Software Measurement

At boot time and at runtime, a HAP device measures software in a trusted manner before that software is allowed to execute.

Separation of Domains

HAP devices leverage the Device Hardware Security capabilities to provide secure separation of domains. Software can be run free from interference or threat from other software running in other domains on the same device.

Remote Attestation

When connecting to a network, a HAP device provides proof of its state to HAP network devices and servers, which can then make a determination about the trustworthiness of the HAP device and, based on that determination, allow access, quarantine or remediate the HAP device.

Secure Central Administration

HAP devices can be administered centrally through their entire lifecycle, enabling the secure provisioning, audit, identification, authentication, management and decommissioning of the HAP devices in enterprise environments.

HAP Technology Goals

The HAP Program promotes commercial development of a broad range of HAP technologies, products and services focused on four key technology goals:

Security

A trusted, measured foundation for service and application infrastructures

Manageability

Centralized administration for the full enterprise lifecycle, including provisioning, audit, management and decommissioning

Sharing

Enforcement of information flow connections across domain boundaries

Form Factor

Support for diverse functionality across a broad range of form factors: desktops, laptops, servers and other devices

For Information Technology Decision Makers

HAP Enhances Cybersecurity

- HAP measures and confirms device integrity to protect networks, information and applications.
- Hardware-based Trusted Computing defeats software attacks.

HAP Technologies Create Savings

- Uses existing hardware – HAP relies on the Trusted Computing Group's Trusted Platform Module (TPM) chip – already on nearly all computers produced today.
- Affordable – HAP can be deployed with commercial, off-the-shelf hardware and software.
- Reduces SWaP – HAP-secured multi-level domain access enables desktop consolidation for a dramatic reduction in hardware and maintenance costs.
- Prevents costly security breaches – with HAP, device integrity is assured for safe data, networks, and applications.

Enhances Network Security

HAP securely stores a device's measurements when it is in a known safe state. Before network access is granted, devices are re-measured and the current state is verified to be in a known, trusted state.

Protects Data from External Threats

HAP securely separates Virtual Machines. With HAP-assured domain isolation, Internet browsing can take place without exposing mission data and applications.

Enables Multi-level Data Access

HAP ensures secure Virtual Machine separation, so single workstations can safely access multiple security domains.

Supports Ad-Hoc Communities of Interest

HAP ensures domain separation and integrity verification, so secure online communities of interest can be quickly and easily established without additional hardware or software.

Monitors Software Integrity

Through ongoing Dynamic Root of Trust Measurement (DRTM), using hardware-based computing, HAP guards against malware and other threats in real-time.

Start Building Trust Now: A HAP Pilot in 3 Steps

Implementing a HAP Pilot offers your enterprise early insight into a vastly more secure and operationally agile future. Commercial off-the-shelf, HAP-based trusted computing technology that's fully certified and accredited is available today to get started.

Step 1: Request a HAP Developer Kit

The HAP Developer Kit includes the information and guidance you need to make the case for trusted computing and the technical insight to know what to do with it.

Step 2: Define a Realistic Trusted Computing Goal

To be successful, start small. Define a modest trusted computing goal where the wins in greater cybersecurity, operational agility, secure virtualized desktops, and/or lower infrastructure costs will be readily apparent and the extrapolated value to the enterprise is large.

Step 3: Build the Trusted Computing Proof Point

Make no mistake: HAP is a paradigm shift. HAP technologies supplant existing desktops, switches, and routers with an interoperable trusted computing architecture. Identify or establish a suitably isolated sandbox where you can reach your goal. Purchase HAP-based technologies off-the-shelf where possible. Engage the HAP Technology Partner Program and knowledgeable HAP Consulting Partners where you need to, to help ensure success.

Request a HAP Developer Kit Now

The HAP Program Management Office (PMO) is making HAP source code and documentation available at no cost to qualified organizations. To request a HAP Developer Kit for your agency or company, email the HAP PMO at hap@nsa.gov.

HIGH ASSURANCE PLATFORM®

Security in a Connected World

www.nsa.gov/hap hap@nsa.gov 410.854.4463

For Technology Vendors, Integrators, OEMs

HAP Enhances Cybersecurity

- HAP measures and confirms device integrity to protect networks, information and applications.
- Hardware-based Trusted Computing defeats software attacks.

New Market Opportunity

- HAP opens a green field of opportunity for vendors to develop component technologies and offer services that leverage and extend HAP-proven standards.
- An opportunity to improve existing solutions and bring to market a broad range of new, more secure solutions for the multi-billion dollar IT security market.

High ROI ➡ High Demand

- HAP combines commercially available technologies with high assurance techniques to affordably deliver an unprecedented level of protection. Government agencies and businesses will find that HAP technologies create savings – easily paying for themselves in improved security and infrastructure costs.

Enhances Network Security

HAP securely stores a device's measurements when it is in a known safe state. Before network access is granted, devices are re-measured and the current state is verified to be in a known, trusted state.

Protects Data from External Threats

HAP securely separates Virtual Machines. With HAP-assured domain isolation, Internet browsing can take place without exposing mission data and applications.

Enables Multi-level Data Access

HAP ensures secure Virtual Machine separation, so single workstations can safely access multiple security domains.

Supports Ad-Hoc Communities of Interest

HAP ensures domain separation and integrity verification, so secure online communities of interest can be quickly and easily established without additional hardware or software.

Monitors Software Integrity

Through ongoing Dynamic Root of Trust Measurement (DRTM), using hardware-based computing, HAP guards against malware and other threats in real-time.

HAP Reference Implementation Standards

The HAP Program is utilizing industry standards and commercial and government best practices to define requirements for HAP components that comply with HAP reference implementation standards. The HAP PMO has identified several key technologies that can be used to develop HAP-compliant solution components.

HAP key technologies include:

- Trusted boot code
- Trusted Platform Module/Mobile Platform Module
- Embedded hardware virtualization security
- Trusted I/O
- Secure virtualization software/hypervisor
- Trusted operating system
- Network access control
- Remote attestation software
- Network encryption
- Remote administration software
- Hard drive encryption

Get Involved

Don’t miss your opportunity to shape the future of cybersecurity. Explore how you can incorporate HAP key technologies into your own solutions. The best way to get started is to request a HAP Developer Kit.

Request a HAP Developer Kit Now

The HAP Program Management Office (PMO) is making HAP source code and documentation available at no cost to qualified organizations. To request a HAP Developer Kit for your agency or company, email the HAP PMO at hap@nsa.gov.

HIGH ASSURANCE PLATFORM®

Security in a Connected World

www.nsa.gov/hap hap@nsa.gov 410.854.4463