Implementing New Hardware-Based Information Security Capabilities

White Paper

The U.S. Defense Intelligence Agency offers a case study for achieving desktop virtualization utilizing Intel® vPro™ technology in year one of a multi-year deployment program.

Author: Michael Mestrovich
Senior Technology Officer for Innovation CCIE #5834
Directorate for Information Management
and Chief Information Officer
United States Defense Intelligence Agency

26 October 2010

Executive Summary

The U.S. Department of Defense (DoD) Defense Intelligence Agency (DIA) is in the first year of a multi-year program to deploy and use Intel® vPro™ technology to support Multi-Level Security (MLS) capabilities on end-user PC desktops enabled with Intel vPro technology and Intel® Graphics. Going forward, DIA looks to build on this effort by implementing a Type 1, bare-metal hypervisor client virtualization solution using Citrix® XenClient™.

The DIA effort is motivated by the need to deliver a secure, cost-effective client environment for defense analysts. Data exploitation and content leakage from IT infrastructure vulnerabilities are leading security concerns for both the private and public sectors. The rapid evolution of cyber-threats requires a flexible technology framework that thwarts adversaries while promoting the organization's ongoing operational efficiency. The burden is increased within the most sensitive portions of the US Government, where the multiplying costs of compartmented data center infrastructures, separate network domains, and multiple client endpoints threaten to exceed the human and capital resources available to manage and evolve them. Without a trusted, end-to-end platform that leverages best-in-breed commercial off-the-shelf (COTS) products, US Government agencies will be constrained in funding and sustaining the defense against the certainty of continued attack; they will also be hampered in fulfilling their mission objectives.

The Department of Defense Intelligence Information System (DoDIIS) client systems currently used by DIA intelligence analysts have limitations displaying computationally and graphically intensive applications at an acceptable resolution. Because modern workloads increasingly call for visually based analysis and collaboration, DIA initiated a search for newer COTS technologies that could enable analysts to better perform their work, and allow the organization to achieve a more reasonable operations and maintenance cost compared to using proprietary or customized solutions. New hardware-assisted virtualization technologies emerging into the marketplace appear promising in their ability to provide high levels of performance and security and greater management ease than was previously possible. The anticipated financial impact is reduced capital expenditures and reduced operational expenditures throughout the enterprise, as well as improved productivity.

Intel vPro technology-enabled PCs provide integrated, hardware-based functionality that may allow multiple operating system environments to reside on each end-user PC desktop or notebook via virtual containers. These capabilities are supported via Intel® Virtualization Technology (Intel® VT) and provide safeguards to protect each virtual environment from malware contamination via Intel® Trusted Execution Technology (Intel® TXT). In addition, new integrated graphics capabilities of the Intel® chipset provide for improved handling of high resolution imagery required by DIA analysts' applications.

This white paper describes new security-oriented technologies that accompany the highest Intel® processor-powered CPUs in the marketplace, enabling a deployment strategy based on a flexible, versatile architecture that will "future proof" the DoDIIS operational environment by accommodating a number of emerging software solutions from industry-leading software companies. This strategy can be implemented at a relatively low cost compared to customized or proprietary solutions.

Contents

Illustrations:

Current DIA Environment

The DIA enterprise faces different challenges in supporting local, branch, and remote users as they perform their assignments and work. Back-end infrastructure, data center consolidation, application development and implementation, data security, and access controls are but some of the moving parts to the ever-developing enterprise. In addition, several common elements make up the enterprise architecture: servers and storage, desktop device, operating systems, LAN and WAN network components, security, identity, encryption, key management, user profile management, and Enterprise Management System(s) monitoring these components.

Currently, with each new mission, DIA requirements dictate a static network architecture in which the applications, operating system, security policies, as well as user profile and access control are all disparately managed. Once established, all component parts become tightly coupled, remarkably inflexible and difficult to patch or update without disrupting the overall design and component parts. Increased man-hours are consumed performing regression testing and ensuring that changes will not affect the mission or create downtime. Add the complexity of regional and remote user needs, and the efficacy of a disjointed and decentralized deployment strategy begins to show its weaknesses.

In most cases, the current DIA enterprise environment is built around deploy-and-locally patch architectures, supporting a number of single and multiple domain solutions. Furthermore, DIA currently supports a multitude of disparate end-point devices. A single enterprise may contain single-domain thick and thin client as well as multiple-domain thin client infrastructures. Support of these different devices is decentralized and requires teams of people to support regional centers.

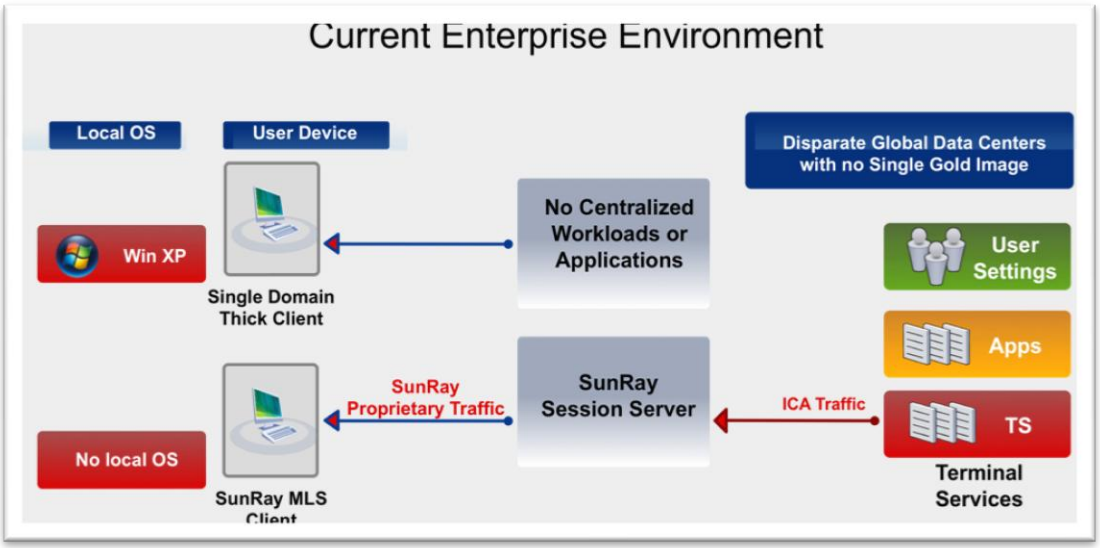

Figure 1: Current Environment State - MLS and Single-Domain Devices

Rising Challenges

The DIA enterprise faces tremendous pressure to provide sustainable, scalable, and secure means by which to provide its users with applications, desktops, and overall global solution management. The advances in technology alone require graphically intensive applications to support analysts, increased resources to provide these applications

as well as desktop management and deployment schedules that must keep up with the changing tides in technology. As a result, desktop maintenance costs, refresh cycles, and sustainment personnel are increasing at multiples that far exceed budgetary and implementation thresholds. To tackle the challenges presented by technology and user requirements, an evaluation is being made of existing commercial off the shelf (COTS) technologies under the Next Generation Desktop (NGD) effort. The outcome of the endeavor can be leveraged across the enterprise for today as well as for the future.

In addition to the challenges presented by data center consolidation, Wide Area Network dependency, and increased collaboration within and outside the agency, a primary challenge facing the US Intelligence Community today is trust. Narrowing down the remarkably complex inter-relationships of today's enterprise is difficult at best, given the multitude of directorates' stove pipe requirements, special access programs, and unique departmental needs – each representing a legacy set of infrastructure and "best practices/ philosophies." Today's users are no longer only connected to their respective LAN; rather they are interspersed across a multitude of networks and security domains, working on differentiated end devices, and may not be employed by the organization within which they operate. The notion of trust extends beyond the user accessing content and onto the requirements of attesting the access device, its operating system, applications, and data, and mitigating the potential threats therein.

Today, DIA leverages a mixture of thick and thin client devices supporting global users accessing, in some cases, upwards of 15 networks on multi security classification domains. With the ever-changing requirement for global management and centralization, as well as graphically intensive applications, the current environment mixture does not provide adequate support for the enterprise user. To properly address an end-to-end solution that can mitigate and resolve the existing problems apparent with the current mesh of thick and thin client devices, license management, application intensity, and back-end infrastructure constraints, this document presents a near-future approach to applying industry-leading technologies currently owned or easily applied by the enterprise, while defining the additional component parts necessary to deliver an enterprise solution to end users.

DoDIIS Environment of the Future (Next Generation Desktop)

In October 2008, DIA initiated a Next Generation Desktop effort. After five years of developing, implementing, and sustaining a government off-the-shelf (GOTS) solution to meet the security requirements imposed on a Multi-Domain solution, DIA's charter of intelligence analysis supporting the US Intelligence Community and Department of Defense eventually grew to rely heavily on the newest collaboration and analysis tools. These tools are based on 3D modeling and computationally intensive applications and simply cannot be supported by the current GOTS platform. Therefore, the primary objectives of the NGD effort have been to:

- Identify COTS solutions that meet or exceed the current security requirements for Multi Domain Access from a single trusted computing platform.
- Provide the most optimal end user experience possible.
- Develop a global enterprise architecture supporting the various user groups, locations, and demands of the DIA Intelligence Analyst.
- Implement an end-to-end solution that leverages the best in client-side to server-side COTS virtualization technologies and the supporting COTS hardware necessary to provide both management and security to the solution.

Through a diligent effort to include all potential, suitable, and viable COTS solutions, DIA sponsored a demonstration of these capabilities in cooperation with MITRE Corporation. The COTS solution providers created a single environment in which the DIA and all elements of the US IC and DOD/ Civilian Agencies could review the various solutions. The technologies reviewed at the MITRE Lab were provided by Microsoft, Citrix, TCS, Sun Microsystems, VMware, Symantec, and Dell Green Hills (now Dell Integrity).

Based on the success of the Lab experience, DIA determined it was feasible to leverage COTS technologies, and elected to move forward with a formalized evaluation of the best possible technology solutions. DIA released an RFP via an existing DIA contract. Upon proposal review, DIA down selected two teams, implementing a pilot evaluation in early 2010, which concluded in June of 2010.

Next Generation Desktop Requirements

Requirements established for the Next Generation Desktop include the following:

- One wire to the desktop computing device that allows the user access to multiple, separate workloads over segregated network domains.
- For security reasons, this requires a trusted operating system wherever there is an aggregation of access on a single device that can be on the back-end or front-end.
- The computing system must support graphics intensive and computationally complex application.
- The computing system must support multicast and unicast video feeds.
- The solution must be scalable and flexible, allowing the DIA enterprise to deploy new capabilities quickly while managing controls centrally by separating the OS, applications, and profile and delivering the user's workload as a service.

Like other IT organizations, the DIA faces the challenge of expanding its capacity and capability in a changing operational and technical environment. The DIA architecture team takes a broad view of all major new deployments and provides technical guidance to ensure that current investments are well aligned with both the existing environment and the long-term strategy. For this program, the goal was to ensure that the client manageability solution was fully integrated into the operations, strategy, capabilities roadmap, and governance framework. Some of the key issues that were considered in defining the solution architecture were:

- Future client hardware and software solutions.
- Emerging technologies and computing models, such as virtualization and streaming applications.
- Data center trends that could impact client management infrastructure.

Next Generation Desktop: A New Paradigm

To achieve the goals of the Next Generation Desktop, the DIA established a new paradigm for client computing, which includes the following characteristics:

- Separate computing elements for user profile, applications and operating system.
- Assemble computing environment dynamically.
- Build from known good master copy of the OS and applications each time.
- Reduce update and patch footprint to one copy of the application or operating system.
- Manage licenses centrally.
- Allow for unique application deployments without negatively impacting the enterprise OS or Standard Workload, enabling the full integration of GOTS applications into a COTS solution.
- Application compatibility to include use of UNIX applications on Windows or Linux Systems, for instance.

Figures 2 and 3 depict the new paradigm for desktop and application delivery, and Figure 4 summarizes the desktop delivery components for the new paradigm.

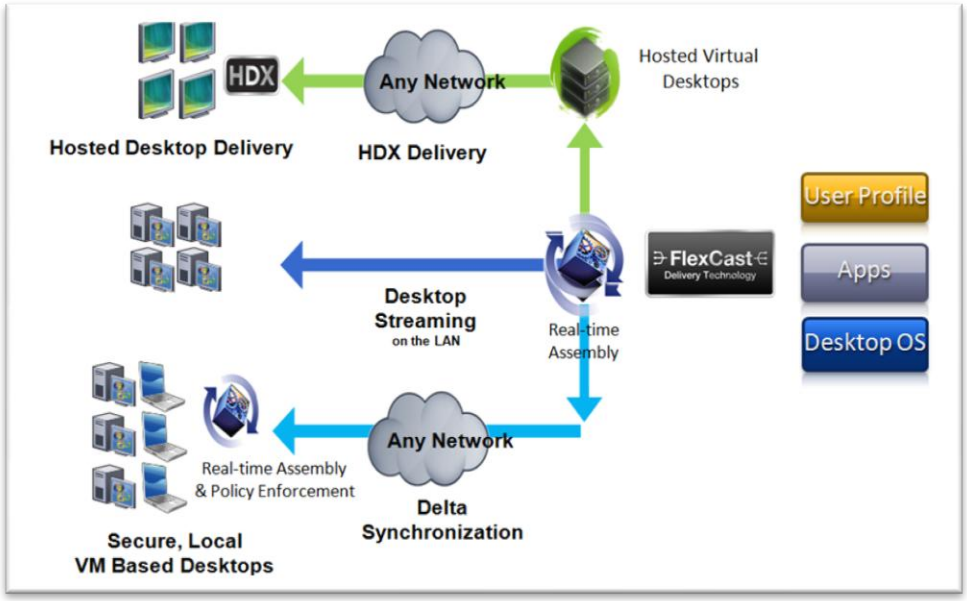

Figure 2. Next Generation Client Computing Paradigm

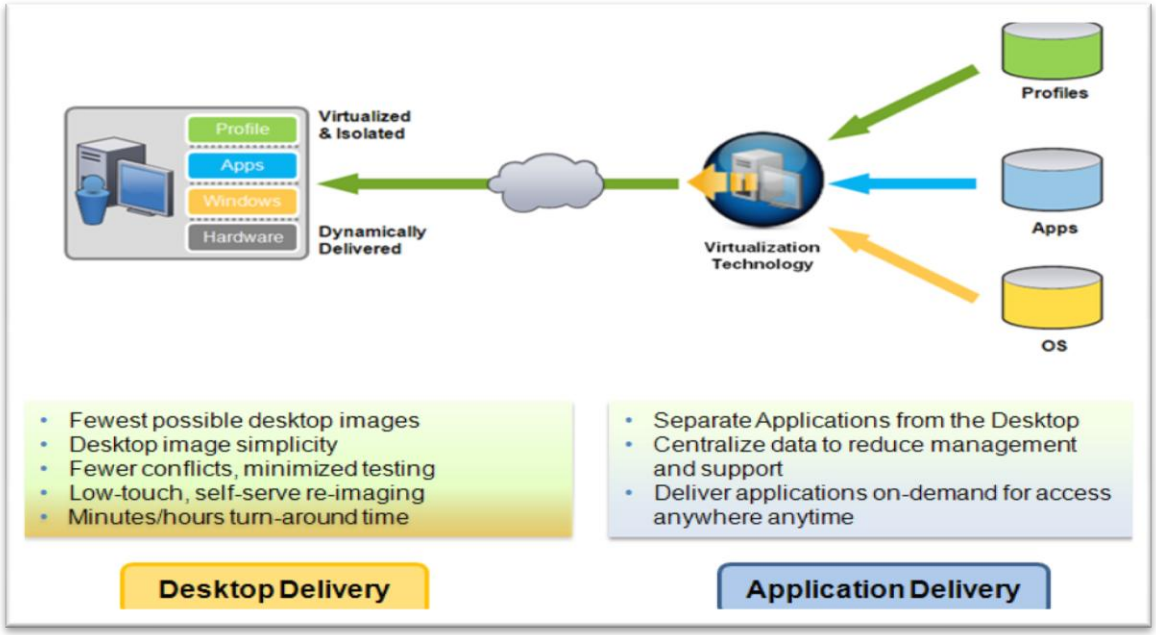

Figure 3. New Paradigm for Desktop and Application Delivery

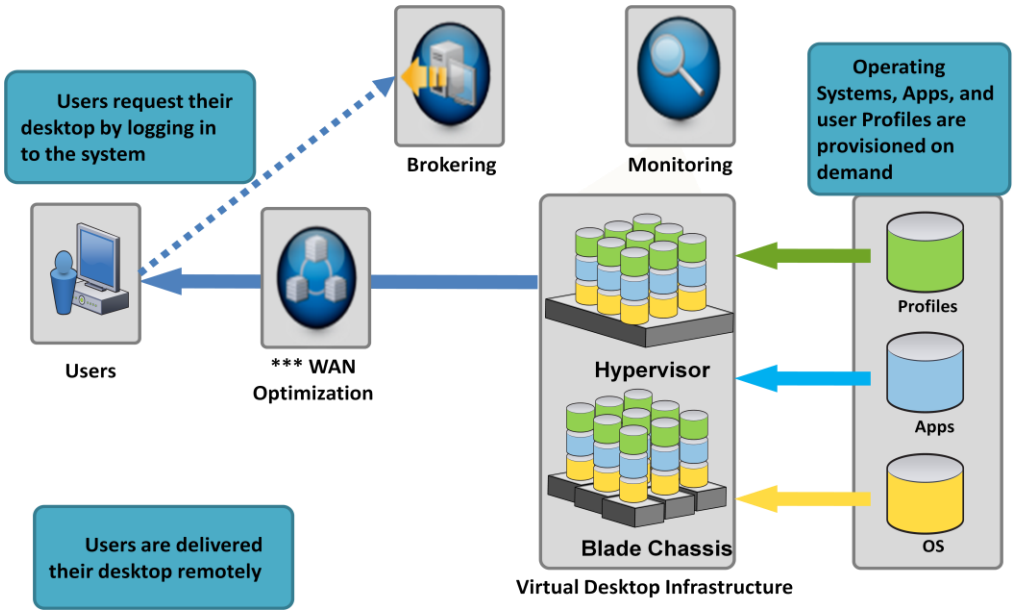

Figure 4. New Paradigm Desktop Delivery Components

NGD Pilot Configuration

After an initial proof-of-concept demonstration, DIA moved forward with a Pilot phase in its assessment of COTS solutions. A down-select was made to two teams, and each implemented its COTS solutions into a live enterprise environment. The two solutions utilized similar backend infrastructures, delivering virtual desktops and applications to their specific end-point device, per domain. Both solutions immediately produced a performance impact over the existing solution, with a reduction in performance latency and increase in user experience with streaming video.

The pilot configuration allowed DIA to leverage an end-to-end delivery architecture that will ultimately enable DIA to utilize Intel vPro technology[1] with an applicable bare metal, Type 1 hypervisor. The current Pilot Delivery Center leverages technologies from Citrix and Intel that will provide the security and performance features necessary to meet DIA's need for a Next Generation Desktop solution.

[1] Intel vPro technology includes powerful Intel® Active Management Technology (Intel® AMT), which requires the computer system to have an Intel® AMT-enabled chipset, network hardware, and software, as well as connection with a power source and a corporate network. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications or implementation of new business processes. With regard to laptops, Intel AMT may not be available or certain capabilities may be limited over a host OS-based virtual private network or when connecting wirelessly, on battery power, sleeping, hibernating, or powered off. For more information, see http://www.intel.com/technology/platform-technology/intel-amt/.

NGD: Leveraging the Investment in Intel® vPro™ Technology

In September 2009, DIA acquired new thick client desktops with the Intel vPro technology stack. The desktops are scheduled to replace existing legacy single-domain machines as well as serve as the basis for the Next Generation Desktop solution end point. DIA expects the Next Generation Desktop effort to produce a solution that fully leverages the security and management attributes of Intel vPro technology-enabled PCs, to include Intel® Trusted Execution Technology (Intel® TXT), Intel® Virtualization Technology[2] for Directed I/O (Intel® VT-d), Intel® Active Management Technology[3] (Intel® AMT), and remote management. The Next Generation Desktop solution shall provide the enterprise with the ability to fully provision a bare metal hypervisor onto the desktop, with central management of the user's workload. The system will leverage not only the security enhancements provided by the COTS platform utilizing Intel vPro technology, but also the built-in capabilities of Intel® Graphics.

Whether supporting a single domain, Multiple Security Levels (MSL), or Multi Level Security environment relying on packet-labeling technologies, the matter of domain access appears to be headed toward a fusion of both MSL and MLS. Moving away from the traditional server-based approach of virtual machines (VMs) to a workload-based system requires a review of network, APIs, and messaging components as they apply to the Delivery Center in its entirety. Since the Type 1 client solution is the final implementation of the Next Generation Desktop infrastructure, customers whose requirements include access to multiple domains will have the ability to centrally manage each user's workload, tie their respective access rights to the applications, and have workloads created and destroyed centrally in real time.

The enterprise's future ability to attest the device prior to network access is key to securing the organization against potential malicious code or defects. Upon login in to the appropriate domain, the user can authenticate against an active list of security domains and have that access matched to their profile list of applications and operating systems. This capability enables the enterprise to tie its internal access controls to profiles and workloads without taxing multiple systems.

The interfaces need to be completely described and enforced via policy. This is increasingly important as the complexity of blended information and usage becomes more pervasive, enabling information of different classifications on a single pane of glass/network wire). A workload-based approach allows for several models:

- Network. This approach uses traditional network controls and management of communications between workloads. A managed virtual switch (vSwitch) coordinates all network activities via organizational policy, even down to endpoint networking. These can be further defined via validated policy to control peer-to-peer

[2] Intel Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM), and, for some uses, certain platform software enabled for it. Functionality, performance, or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

[3] No computer system can provide absolute security under all conditions. Intel Trusted Execution Technology (TXT) is a security technology that requires for operation a computer system with Intel® Virtualization Technology, an Intel Trusted Execution Technology -enabled Intel processor, chipset, BIOS, Authenticated Code Modules, and an Intel or other Intel® Trusted Execution Technology compatible measured virtual machine monitor. In addition, Intel Trusted Execution Technology requires the system to contain a TPMv1.2 as defined by the Trusted Computing Group and specific software for some uses. See http://www.intel.com/ for more information.

networking between VMs.

- API's. Programs and agents interact directly with each other via programmatic interfaces. This requires API support within the workload and/or introspection from external agents. Open, carefully reviewed, and white-listed API calls, parameters, and results are essential to verified security.
- Messaging. An authenticated message-passing interface is enabled in workload components. Individual actions can have their own authentication requirements, which can even require multi-factor external validation and approval for escalations, emergency access, and exceptions.

These methods can be layered to provide for Defense in Depth. Expressing the policy to specify, control, and audit the desired and undesired activities drives the usability and overall security posture of the model.

Implementing Security

One of the most important issues was integrating the new DoDIIS Solution with existing security policies to ensure secure client management across the enterprise. This required that new client technologies be available to support virtualized operating systems within the context of a trusted computing environment. Specifically needed are Intel Virtualization Technology (Intel VT) and Intel Trusted Execution Technology (Intel TXT). Advanced Encryption Standard New Instructions (AES-NI) were an additional benefit.[4]

Intel® Virtualization Technology (Intel® VT)

Intel Virtualization Technology makes a single system appear as multiple independent systems to software. This allows multiple, independent operating systems to run simultaneously on a single system. Intel VT comprises technology components to support virtualization of platforms based on Intel® architecture-based microprocessors and chipsets. Intel Virtualization Technology (Intel VT-x) includes added hardware support in the processor to improve the virtualization performance and robustness. Intel Virtualization Technology for Directed I/O (Intel VT-d) adds chipset hardware implementation to support and improve I/O virtualization performance and robustness.[5]

Intel® Trusted Execution Technology (Intel® TXT)

Intel Trusted Execution Technology defines platform-level enhancements that provide the building blocks for creating trusted platforms. The Intel TXT platform helps to provide the authenticity of the controlling environment so that those wishing to rely on the platform can make an appropriate trust decision.[6]

The Intel TXT platform determines the identity of the controlling environment by accurately measuring and verifying the controlling software. Another aspect of the trust decision is the ability of the platform to resist attempts to change

[4] AES-NI is a set of instructions that consolidates mathematical operations used in the Advanced Encryption Standard (AES) algorithm. Enabling AES-NI requires a computer system with an AES-NI-enabled processor as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on Intel® Core™ i5-600 Desktop Processor Series, Intel® Core™ i7-600 Mobile Processor Series, and Intel® Core™ i5-500 Mobile Processor Series. For further availability of AES-NI enabled processors or systems, check with your reseller or system manufacturer. For more information, see http://softwarecommunity.intel.com/isn/downloads/intelavx/AES-Instructions-Set_WP.pdf.

[5] Intel VT-x specifications and functional descriptions are included in the Intel® 64 and IA-32 Architectures Software Developer's Manual, Vol 3B, available at: http://www.intel.com/products/processor/manuals/index.htm

[6] The Intel VT-d specification and other VT documents can be referenced at http://www.intel.com/technology/virtualization/index.htm. Information about Intel TXT and other security technologies can be found at http://www.intel.com/technology/security/

the controlling environment. The Intel TXT platform resists attempts by software processes to change the controlling environment or bypass the bounds set by the controlling environment.

Intel TXT is a set of extensions designed to provide a measured and controlled launch of system software that will then establish a protected environment for itself and any additional software that it may execute. These extensions enhance two areas: launching the Measured Launched Environment (MLE), and protecting the MLE from potential corruption.

The enhanced platform provides these launch and control interfaces using Safer Mode Extensions (SMX). The SMX interface includes the following functions:

- Measured/Verified launch of the MLE.
- Mechanisms to ensure the above measurement is protected and stored in a secure location.
- Protection mechanisms that allow the MLE to control attempts to modify itself.

Advanced Encryption Standard New Instructions (AES-NI)

With AES-NI, six new Single Instruction Multiple Data (SIMD) instructions are introduced on the processor. These instructions enable fast, secure encryption and decryption using the Advanced Encryption Standard. Four of the instructions (AESENC, AESENCLAST, AESDEC, and AESDELAST) facilitate high performance AES encryption and decryption. The other two, AESIMC and AESKEYGENASSIST, support the AES key expansion procedure. Together, these infrastructures provide full hardware support for AES, offering security, performance, and flexibility.

Intel® Graphics

DIA's current DODIIS environment is hindered due to the poor graphics display qualities of the aging hardware solution. Intel® HD Graphics provides outstanding visual performance for sharper images, richer color, and lifelike video. Analysts can view videos in high definition and get full support for Microsoft® Windows® 7. There's no need for an extra add-in graphics card, since full graphics and media support are already built-in. Intel HD Graphics is available on select models of the 2010 Intel® Core™ processor family.[7] Depending on system configuration and vendor support, users can switch between integrated graphics and discrete graphics on the fly, gaining more performance for intense graphics workloads with no reboot necessary.

[7] For more information, see http://www.intel.com/products/graphics/index.htm

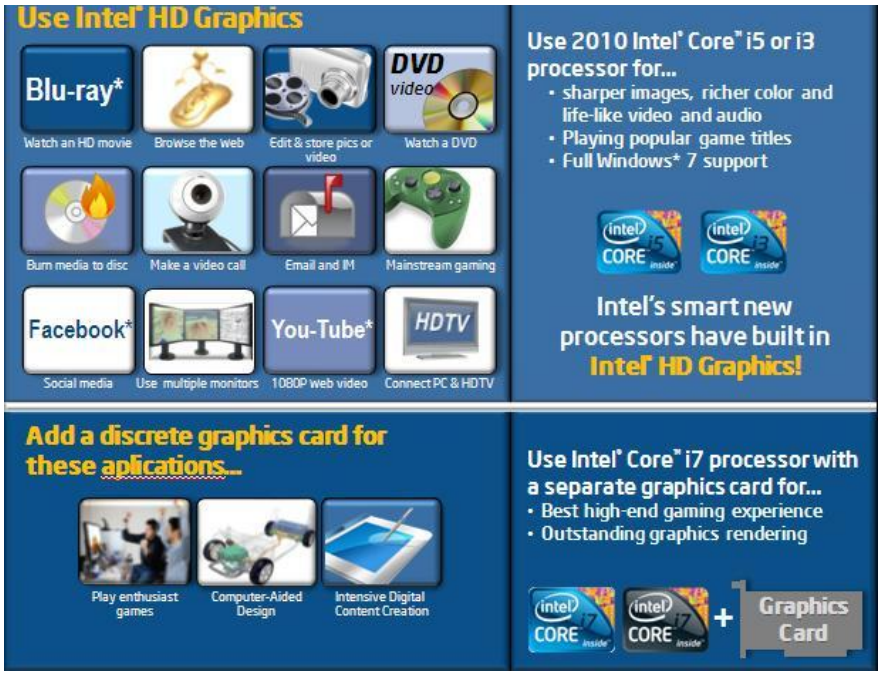

Figure 5. Intel HD Graphics Summary

The Path Forward: Virtualizing the Rich Client Environment

With its investments in Intel vPro technology, DIA hopes to leverage the NGD effort to ultimately implement a true Next Generation Desktop solution based on a Type 1, bare metal hypervisor platform.

In January 2009, Citrix announced a formal agreement to develop a Xen®-based bare-metal client hypervisor technology in conjunction with Intel.[8] The result of the collaboration is Citrix® XenClient™, a local desktop virtualization platform that provides new levels of security and user flexibility for enterprise desktops.

XenClient enables IT administrators to deliver each employee's corporate desktop as a secure virtual machine that runs directly on that user's computer. XenClient ensures that corporate applications and data are completely isolated from personal data, greatly increasing security and simplifying regulatory compliance. New desktop deployments, hardware upgrades, and employee moves are less of a problem, since IT administrators can quickly deliver a new desktop or move an existing one to any XenClient enabled device. Because the desktop and applications execute locally, users are free to work online or offline with all the rich performance experience of a traditional computing environment.

Citrix XenClient Overview

The goal of client virtualization is to provide secure desktops with the flexibility and freedom users require to carry out their computing needs. XenClient enables this vision by taking advantage of Intel vPro technology—a collection of powerful manageability solutions found on select Intel® Core™ i5 and Core i7 processors. Intel vPro technology

[8] http://www.citrix.com/English/ne/news/news.asp?newsID=1685762

provides enhanced security and manageability; it also improves remote maintenance both inside and outside the firewall through Intel Active Management Technology (Intel AMT), a component of Intel vPro technology. Intel AMT enhances PC manageability with hardware-based capabilities to help administrators discover, heal, and secure their networked computing assets. Administrators can diagnose software and hardware problems more accurately, regardless of the PC's power state.

These capabilities enable dramatic cost and energy savings through out-of-band management, remote troubleshooting, asset tracking, power on/off, and more. With XenClient, devices, desktops, applications, and people can operate more independently while retaining the security and other benefits of centralized management.

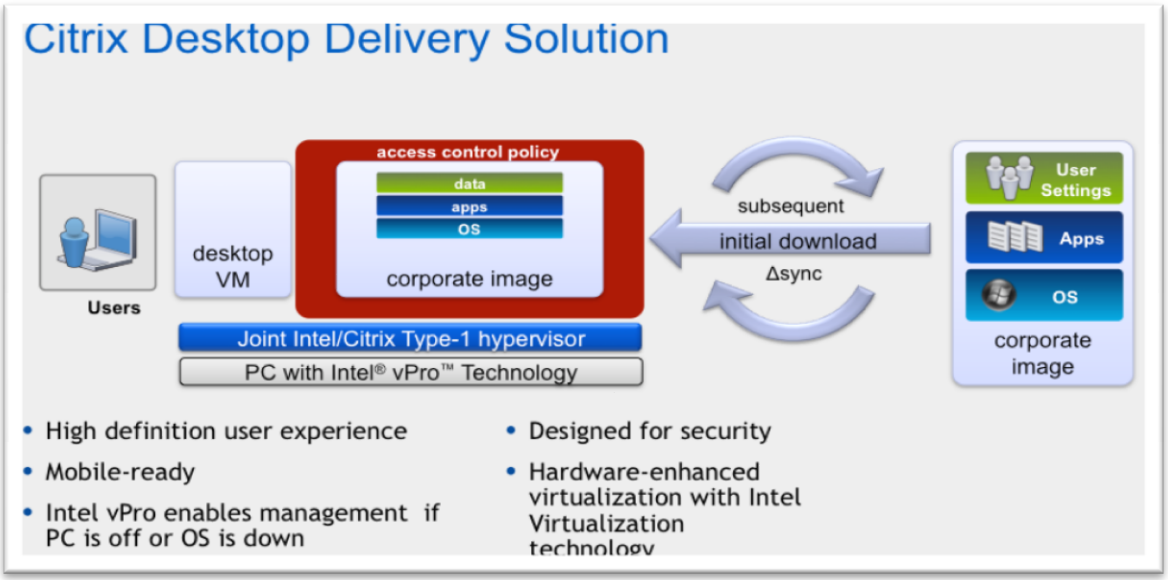

Figure 6. Citrix Desktop Delivery Solution, Enhanced with Intel VT

Outstanding Performance with the XenClient Hypervisor

At the heart of this vision is the XenClient hypervisor—a bare-metal hypervisor that runs directly on device hardware by using Intel VT hardware-assisted virtualization technology, a component of Intel vPro™ technology.

Intel VT is foundational to the Xen approach—the same mature Xen approach that is used in the Citrix® XenServer™ server virtualization platform. Two distinct aspects of Intel vPro technology play important roles:

- Intel VT-x provides CPU virtualization support and performance enhancements, and is required by Xen to run VMs running the Windows® operating system.
- Intel Virtualization Technology for Directed I/O (Intel VT-d) allows for direct and secure assignment of devices to VMs, reducing overhead and increasing the overall reliability of the platform.

XenClient leverages these and other capabilities of Intel vPro technology to improve the user experience with the virtualized desktop.

Intel® Hyper-Threading Technology makes higher throughput possible on multi-threaded software running on the virtual desktop, and Intel® Turbo Boost Technology allows processor cores to run faster when workload demands it. Furthermore, the integrated memory controller in Intel® Core™ i5 and Core™ i7 vPro™ processors offers stunning memory read/write performance. With these and other features, users get the performance and flexibility they expect from a desktop while the organization reduces desktop-related energy costs.

The use of Intel vPro technology with XenClient lets local VMs run at maximum performance and gives users the productivity benefits of a rich desktop experience. While client virtualization solutions have existed for years, they have primarily used emulation software—a hardware emulation application that is installed on top of a base operating system to enable the hosting of the guest VMs. Virtualization based on hardware emulation generally results in degraded performance of guest VMs and a poorer user experience.

Tight Security with XenClient

In addition to superior performance, XenClient bare-metal virtualization provides higher levels of security through the isolation of guest VM resources. As a Type 1 bare metal hypervisor, the XenClient hypervisor runs directly on device hardware (Figure 7, right side).

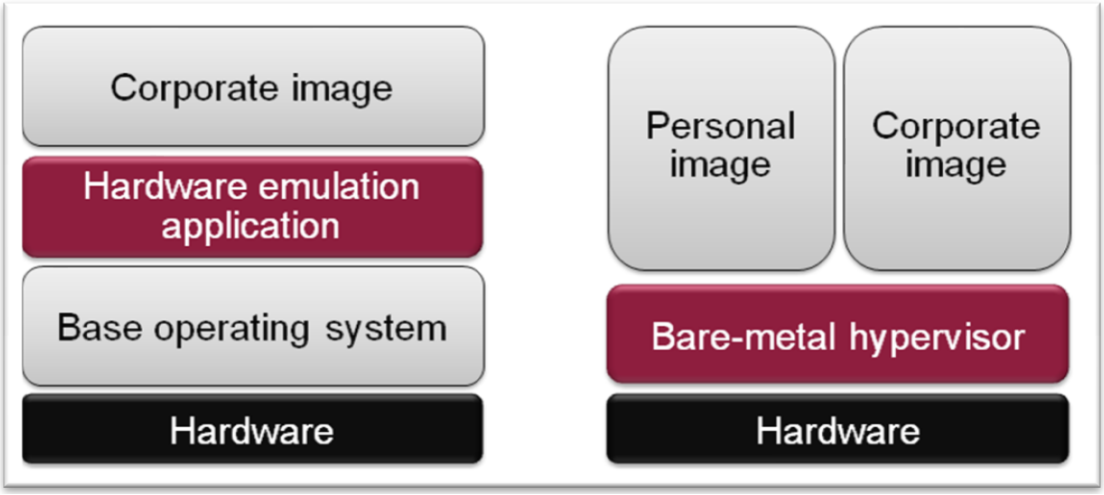

Figure 7. Type 2 vs Type 1 Hypervisor

This level of isolation enables organizations to give users a choice of running both business and personal environments on the same device, or multiple business workloads supporting different aspects of the enterprise, in isolation, without fear that personal applications and data are putting business environments at risk (Figure 8). For example, a business VM could be locked down and tightly managed, with users unable to install applications. A personal VM could allow local administration while disallowing access to corporate networks or data. The user can easily and securely switch between these VMs.

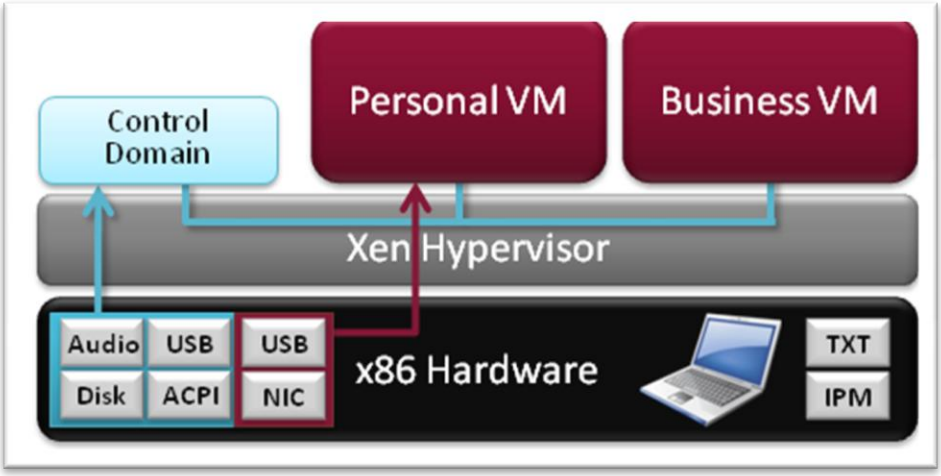

Figure 8. Citrix XenClient Use of Intel VT and Intel vPro Technology

XenClient uses Intel TXT to enhance VM security. Intel TXT lets the hardware verify the integrity of the hypervisor and its support components on every boot so that the hypervisor becomes part of the trusted compute base. Intel TXT forges a chain of trust from the hardware up to the virtualization layer, helping ensure that the hypervisor has not been compromised.

With emulation-based virtualization solutions, if the base operating system is compromised, the VMs running on top of it are subject to compromise. In contrast, with XenClient and Intel TXT, the guest VMs running on XenClient become part of a trusted execution environment and remain isolated from each other, so that performance or security issues within one environment do not affect other desktop environments on the system.

Yet another benefit of Citrix and Intel collaboration on XenClient local desktop virtualization is hardware-independent desktop images. The XenClient hypervisor creates an abstraction layer between the device hardware and the guest virtual machines. Consequently, a single disk image can be used on different types of devices. IT administrators can supply users with local VM-based desktops, regardless of the hardware on which the device is running. This creates truly hardware-independent VMs that can be moved between different versions of desktops or laptops from one vendor or between machines from different vendors, reducing the burden of managing multiple operating system images to cover heterogeneous hardware.

Additional Capabilities of Citrix XenClient and Intel vPro Technology

XenClient with integrated Intel vPro technology also enables out-of-band management and policy enforcement. For example, a user can apply updates at the hypervisor level, where, because it is outside the operating system, it is more secure and more efficient. In the future, some functions that have traditionally been performed inside the operating system, such as malware detection, backup, and virtual private network (VPN), can be handled at the hypervisor level in a more robust and secure fashion. For example, running a VPN outside the operating system avoids exposing the cryptogram key (which is necessary for a VPN) to the guest operating system, enhancing security.

Users can also map devices, such as graphics cards, directly into the VM in a process called hardware pass-through. This process enables a full, high-definition user experience within the VM. With maximum flexibility and performance, XenClient provides a new way to deliver desktops through a mix of total isolation and sophisticated device pass-through. The technology enables new use cases for rich client execution while applying client virtualization, delivering all the benefits of centralized management and delivery of desktop workloads and applications to users.

Conclusion

Today's operating environment within the Intelligence Community is becoming ever more complex. As our international partnerships and commitments grow, the information systems that support those alliances must also expand. The nature of intelligence is that it must only be shared with those who have a "need to know." In the past, expanding international relationships and the subsequent sharing of intelligence information necessitated the creation of separate networks and all the various infrastructure that would accompany them, such as storage systems, switches, and routers, PCs, servers, and so forth. The Next Generation Desktop effort is an effort to provide a multi-security level access device that obviates the need for those multitudes of distinct network infrastructures.

The current state of technology has been shown to support the goals of the Next Generation Desktop; that is, to provide a single desktop device, either thick client or thin client, that can access a multitude of different classified networks and still process today's most demanding multimedia, geospatial, and computationally complex applications. The modern realities of desktop and application virtualization have made it possible to support these demanding applications in a cost-effective fashion.

The movement toward thin clients was an effort to reduce the overhead of traditional PC management and reduce the threat associated with managing thousands of end stations running a well-known and well-exploited operating system. Effective patch management became an ever-increasing issue as the speed with which security threats and exploits accelerated. But thin client computing failed to provide the necessary support for modern multimedia-based applications. Today's advances in virtualization and solutions such as Intel vPro technology look to provide for us the best of both worlds: the power of the traditional PC coupled with the ease of management and heightened security of thin client infrastructures. The Type 1 hypervisor creates an optimal operating environment and is the state of operation envisioned as the future for our Next Generation Desktop computing environment.

However, the Next Generation Desktop is not only about an end client computing device. The NGD is also, and perhaps most importantly, about restructuring the way applications and desktops are delivered and managed by the enterprise. By centralizing desktop management and by abstracting the application from the underlying OS, a robust and reliable operating environment is created. The ability to effectively patch desktop OSes increases while reducing the time and manpower necessary to create that heightened patch compliance. This removes the need to regression test applications against various OS baselines as the applications are virtualized and abstracted from the operating system. All of this allows for a much more dynamic application and system delivery environment that can only help the end customer in the ever-evolving war on terrorism.

Author

Michael Mestrovich
Senior Technology Officer for Innovation CCIE #5834
Directorate for Information Management and
Chief Information Officer
Defense Intelligence Agency

Acronyms

AMT	Active Management Technology
API	Application Programming Interfaces
COTS	Commercial Off-the-Shelf
GOTS	Government Off-the-Shelf
MLS	Multi-Level Security
MSL	Multiple Security Levels
NGD	Next Generation Desktop
OS	Operating System
TXT	Trusted Execution Technology
VPN	Virtual Private Network
VT	Virtualization Technology
VT-d	Virtualization Technology for Directed I/O