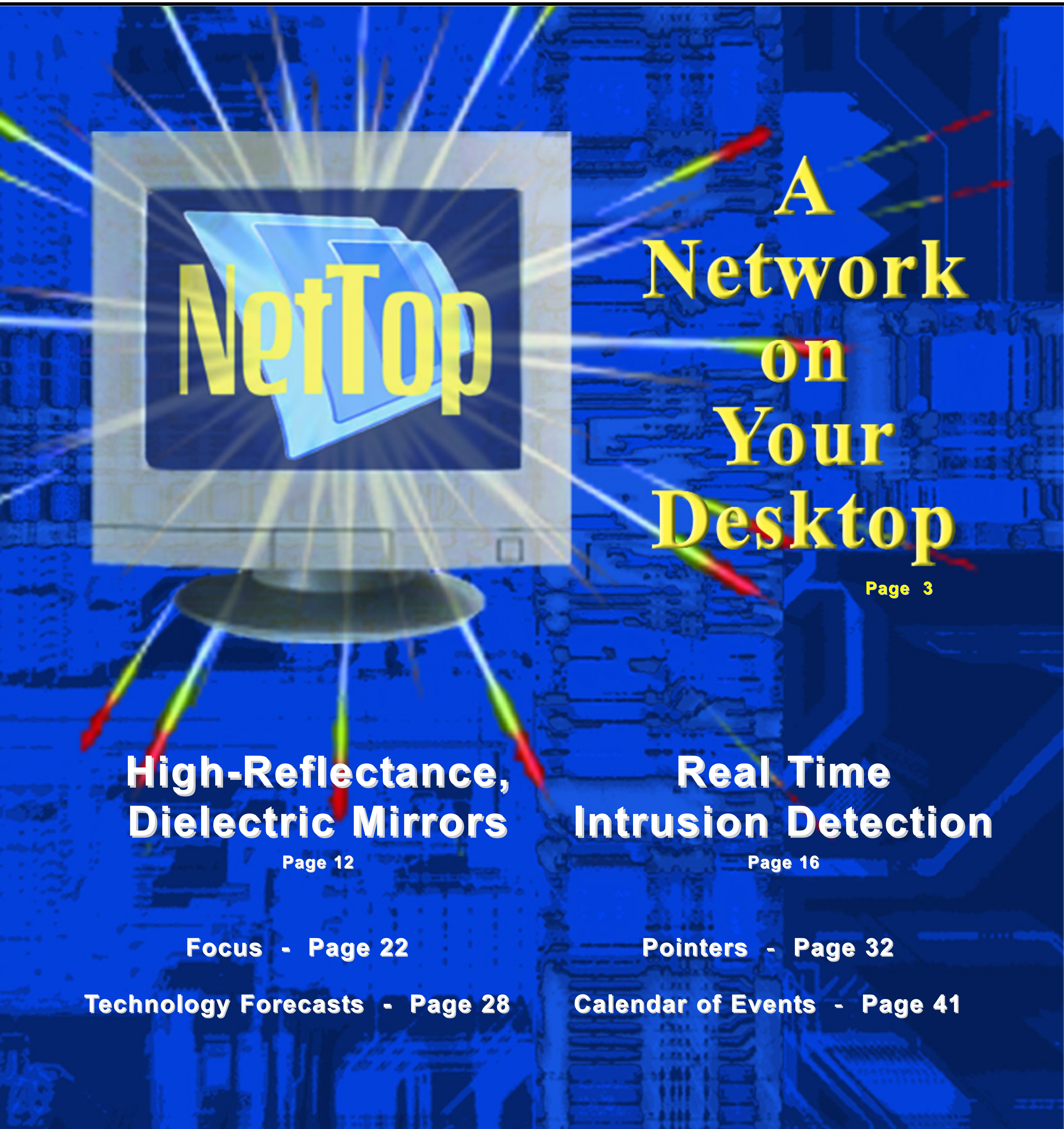
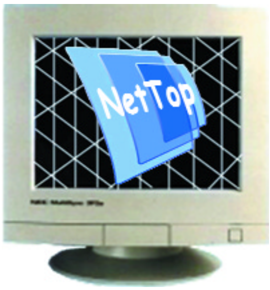
Tech Trend Notes

Preview of Tomorrow's Information Technologies

Volume: 9 Edition: 4 Fall 2000





NetTop

Commercial Technology in High Assurance Applications

By Robert Meushaw and Donald Simard

Introduction

The decade of the nineties has been particularly challenging for the National Security Agency's Information Assurance mission. The gradual but accelerating changeover from government produced technologies to commercial products and services has seriously eroded our ability to protect information processed by the national security community. Numerous government programs intended to produce high assurance data systems and workstation platforms have been largely unsuccessful, and the buying power of the government has not commanded the attention of the IT industry. The historical flow of technology from government to industrial and home users has largely been reversed. We often find technologies that are more sophisticated in our homes earlier than in our government workspaces. The shortcomings of our information assurance technologies are further evidenced by the shift of R&D resources away from protection and into detection and response initiatives.

To address these issues, during the summer of 1999 the NSA Advisory Board (NSAAB) reviewed the Information Systems Security Organization's (ISSO) commercial-off-the-shelf (COTS) strategy. The board acknowledged the need to provide the functionality and the feel of familiar COTS technology to our users, but they believed that we would not be able to influence the security of COTS technology for high assurance applications. The board challenged the Information Assurance Research Office to initiate a project to develop architectures that would allow COTS technology to be used safely in high assurance applications.

A Tiger Team was assembled for a one-year effort to develop an architectural approach to allow the safe use of COTS in sensitive Government applications. The user should see a familiar interface, e.g., Microsoft Windows Operating System (OS) and off-the-shelf application software, but achieve the assurance needed for DoD use. The NSAAB suggested that one or more government-off-the-shelf (GOTS) components be included, preferably as plug-ins; and their removal should allow the system to be used as a normal COTS machine. The notion of a "Vault" was introduced as an Internet accessible, protected enclave that would provide high assurance services to connected user machines.

The results of the Tiger Team effort are a proof-of-concept architecture and a set of components that are referred to as NetTop. The remainder of this article will describe the concept and technical approach used in the architecture, identify several investigated applications, and suggest future capabilities.

User Requirements

The ISSO's customers have long identified shortcomings with the security technology that was available to them. One significant concern is that their workspaces are cluttered with computer equipment to support access to multiple networks of differing sensitivity. Dealing with this duplication of equipment has long been a problem, since there is no single system that can support all of their access needs. A second concern is that government developed security solutions have often been incompatible with other standards-based IT products, which has significantly complicated the interfacing and upgrading of system components. The cost and complexity of network management is also a steadily growing issue, particularly in times of declining resources and mounting security concerns over the outsourcing of support. Our customers also need the ability to move data across isolated networks in order to perform their daily tasks, and the techniques to make such transfers efficient and safe. Finally, the increased importance placed on coalition operations brings new challenges for technology to securely support these operations. The architecture of the NetTop prototype suggests a near-term approach that can provide a useful and practical set of capabilities to satisfy these needs.

An Initial Capability

To begin the development of the NetTop architecture, a modest, initial capability was sought. Opportunely, the ISSO's System Solutions Group identified an Internet-based version of the Remote Access Security Program (RASP) system as an excellent prospect. The RASP provides secure remote access to a host computer over a dial-up connection, and includes a laptop computer and a specially developed encrypting modem to protect the communications link. Many customers have requested a similar capability for remote network connectivity, but using Internet connections through a local Internet Service Provider (ISP), i.e., use the public data network rather than the public voice network. The ability to provide a secure, remote connection over the Internet to a secure enclave was selected as the initial NetTop goal.

An architecture that can achieve this capability has been known for some time. It typically includes an end-user workstation, an in-line encryptor, and possibly a filtering router or firewall to connect to the Internet. Commercially, such solutions are knows as Virtual Private Networks (VPN). Figure 1 depicts a typical VPN client configuration. This system configuration would provide the required functionality, but it would be cumbersome and expensive for a mobile user.

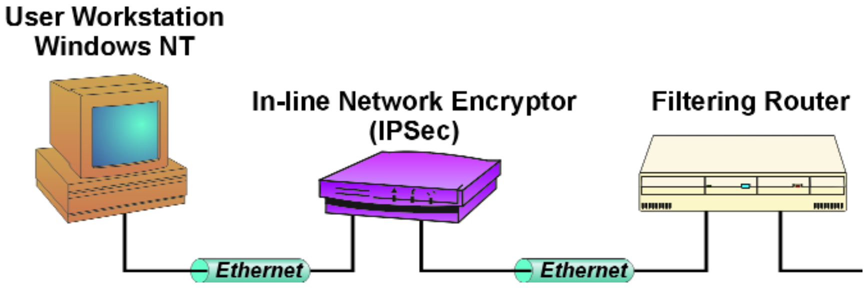


Figure 1 - Typical Virtual Private Network Client Configuration

Recycling Technology

The requirement that NetTop users see a familiar COTS computer desktop environment was taken as a fundamental precept of the architecture. One consequence of this approach is that for high assurance applications, the end-user environment must be presumed to be untrustworthy, and the NetTop architecture must protect against potentially hostile behavior.

In order to place limitations upon a potentially malicious component, we explored the concept of encapsulation to constrain the behavior of the end-user operating system and application software. The method selected for encapsulating the OS was based upon a 30-year-old technology, Virtual Machine Monitors (VMM). VMM technology was designed and developed in the era of large IBM mainframe computers, and was intended to help extend the life of legacy software, when improved hardware or OS software was released. In essence, a VMM was a software system that ran directly on the computer hardware, and allowed multiple operating systems to be installed on top of it. By running older OS versions in some virtual machines, legacy software could be run, while newer application software could be executed in VMs running more current OS versions.

Commodity VMMs

During the NetTop design discussions, we identified a new commercial product, VMware, that provided a practical VMM capability. The VMware product is a spin-off of DARPA-sponsored research at Stanford University, and is generally used for providing a safe test environment for OS and networking software.

There were several novel capabilities of VMware that made it attractive for use in NetTop. First, it was designed for efficient operation on Intel x86 platforms rather than on large mainframe computers, which made it suitable for use on commonplace personal computers, workstations, and laptops. Next, VMware operates on top of an underlying host OS rather than directly on the system hardware. VMMs that run directly on hardware have been studied previously under Project Neptune for their use in securing systems. A Neptune type of VMM would face the enormous challenge of keeping pace with changes in the underlying hardware platform. VMware takes advantage of the host

OS's need to track these changes. This is a much more practical approach, and would be particularly important to produce a GOTS VMM for NetTop. Lastly, VMware provides an abstraction for "virtual Ethernet hubs." This capability allows virtual machines to be interconnected in a fashion that is well understood by network designers and administrators.

A Network on a Desktop

Using VMware, the initial NetTop system was constructed using a powerful laptop computer. The operating system chosen for the host OS was Redhat Linux Version 6.2. Three virtual machines networked by two virtual hubs were installed on top of the host OS, providing an in-line configuration of three machines comprising (1) an end-user Windows NT machine, (2) an encrypting machine using IPSec, and (3) a Filtering Router (FR) machine. Both the VPN and FR were hosted on VMs running the Linux operating system. Figure 2 displays the initial NetTop prototype configuration.

The initial NetTop configuration demonstrates a number of important capabilities. It encapsulates the unmodified, end-user Windows operating system in a VM. An important characteristic of this approach is that the encryption can be provided as an in-line function that cannot be bypassed by malicious actions of the end-user OS or application software. Rudimentary protection from network attacks is provided through a filtering router.

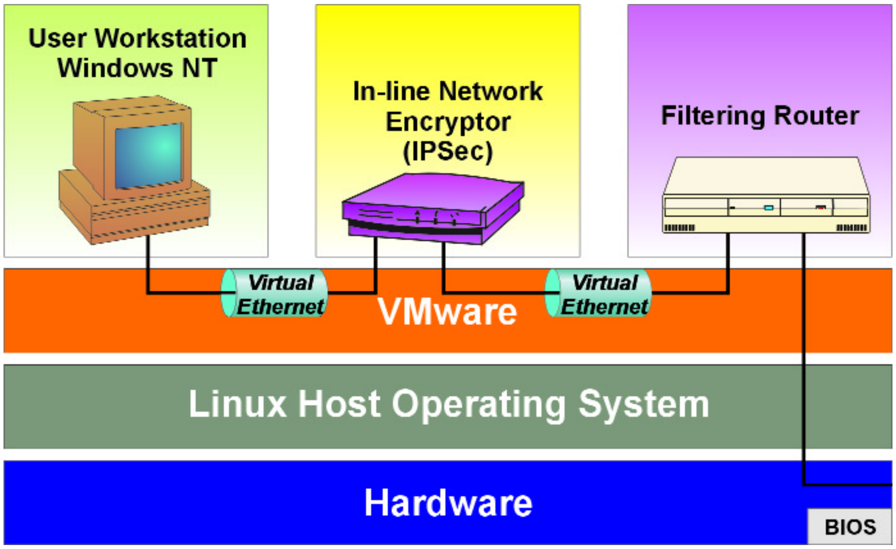


Figure 2 - Simple NetTop System Configuration

Any of the individual virtual machines can be replaced or upgraded with standards-based components. The interconnection of the virtual machines is based upon familiar TCP/IP networking. Finally, a single platform replaces several traditional components, thereby reducing hardware and maintenance costs. An important side benefit is that the architecture makes no assumptions about the communications technology used to connect the external network. The user is free to select the desired technology, including dial-up, Ethernet, ATM, wireless, etc.

The basic NetTop configuration provides the same functionality as three separate hardware platforms. Each virtualized component should operate identically to its real-world counterpart with "bug for bug compatibility." The simple NetTop configuration was successfully connected across the Internet to a simulated, secure enclave on an unclassified NSA network, using both dial-up

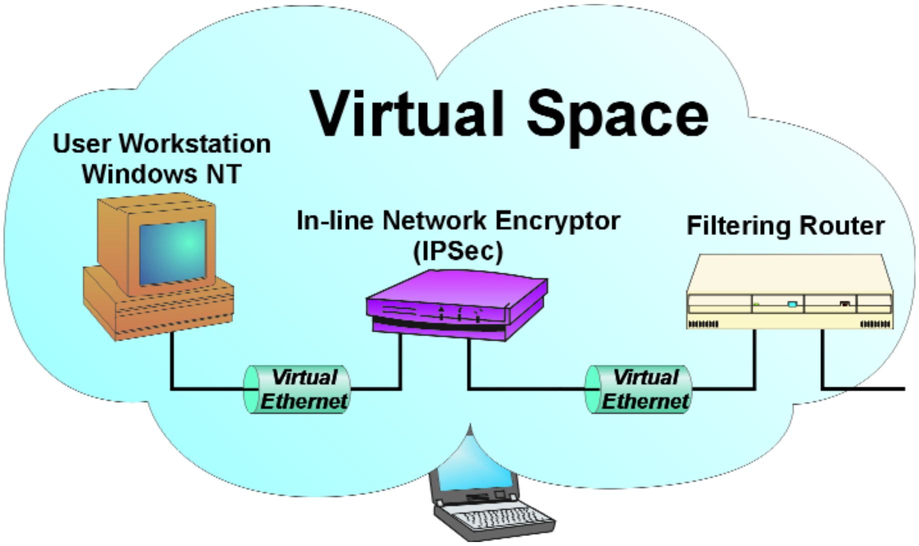


Figure 3 - NetTop Logical Configuration

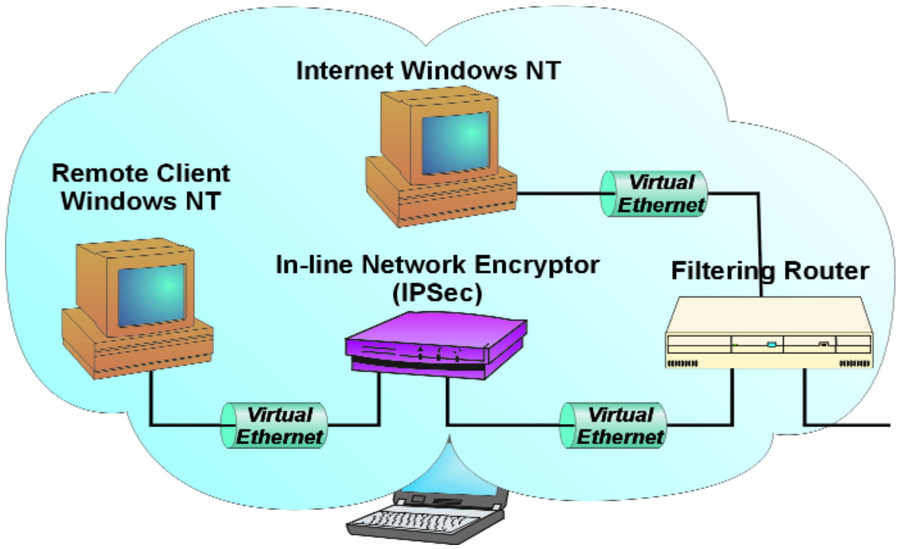


Figure 4 - NetTop Multiple Security Level Configuration

and cable modem connections. Such a configuration could have all of the capabilities of a locally connected machine, including the ability to connect to the Internet, if permitted within the enclave. Figure 3 illustrates a NetTop logical configuration.

Multiple Security Levels

A natural extension to the first prototype was the addition of other VMs to provide increased functionality. The second version of the NetTop prototype included another Windows NT machine connected directly to the filtering router as shown in Figure 4. This machine allows a user to access the Internet directly. This extended prototype suggests a powerful feature of the NetTop architecture - the ability to replace multiple end-user workstations within a single, hardware platform. In theory, multiple user connections to networks of differing sensitivity could be provided using multiple VPNs. This environment provides Multiple (single) Security Level (MSL) capability rather than true Multi-Level Security, but still addresses an important customer need.

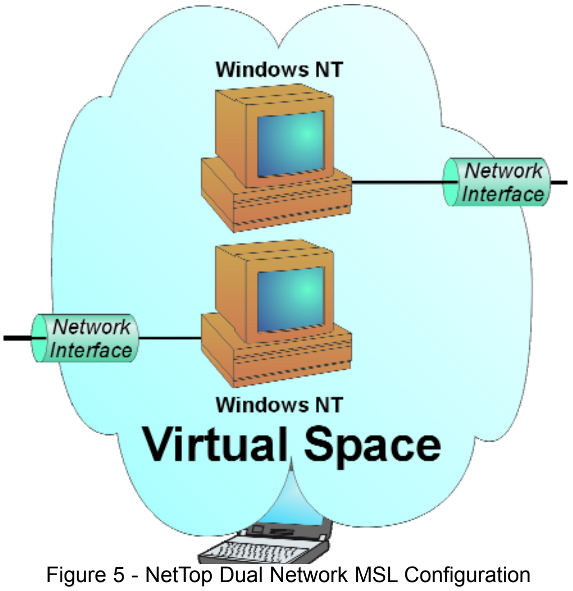


Figure 5 - NetTop Dual Network MSL Configuration

Another configuration for a MSL system is shown in Figure 5, where two isolated VM workstations are connected to two different networks through two network interface cards. Since the network connections are already physically isolated, encrypted communication tunnels are not needed. This type of NetTop configuration may be appropriate to replace multiple end user workstations, when separate communications infrastructures are already available.

Thin-Client VMs

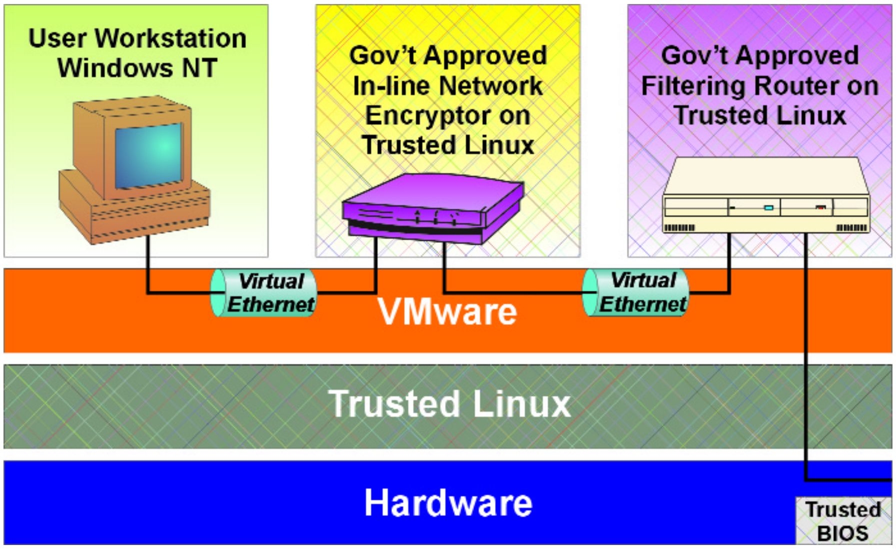
While the VMs described so far have been fully configured Windows or Linux systems, there is nothing preventing a VM from being a "thin client." In fact, there may be reasons why a thin-client would be preferable. For example, if the Windows NT in Figure 4 was installed as a "display only" thin-client, all classified files could be kept on a remote server in a protected enclave. This configuration increases assurance, since the NetTop device contains minimal sensitive information.

Assurance

Despite the functional and cost advantages that the NetTop architecture described above may offer to some users, its usefulness will depend upon its ability to withstand determined attacks from the external network and from malicious end-user software. The most sensitive applications may require additional protection against compromising system failures. While NetTop attempts to deal with insecurities that may be caused by user errors, no attempt has been made to thwart malicious insiders. As a practical matter, it should only be necessary to demonstrate that a NetTop configuration provides the same degree of security as the separate network components that it replaces. If this can be achieved, then the basic architectural approach is validated.

A number of approaches have been identified to increase the assurance of the NetTop architecture. The critical aspect of the architecture that must be validated is the ability of the VMM/Host OS combination to sufficiently isolate the various NetTop components. Our approach to dealing with security in the underlying host is to use a Trusted Linux OS prototype that has been developed under the IARO's OS Security research program. Trusted Linux incorporates flexible access control mechanisms. In order to bolster the inherent isolation provided by the VMM, a tailored security policy has been developed for the Trusted Linux host. The VMM/Trusted Linux combination will be evaluated further during an internal "red team" exercise to assess the degree of isolation it provides.

The Trusted Linux prototype is also envisioned for use as the guest OS in the VPN and Filtering Router VMs. It is likely that a substantially reduced Trusted Linux OS could be configured to support each VM. In each case, specific security policies need to be tailored to support the limited functionality of each machine. The particular encryption and filtering router products selected could be from National Information Assurance Partnership approved lists or specially developed GOTS components.



User Workstation Windows NT
Gov't Approved In-line Network Encryptor on Trusted Linux
Gov't Approved Filtering Router on Trusted Linux
Virtual Ethernet
VMware
Virtual Ethernet
Trusted Linux
Hardware
Trusted BIOS

Figure 6 - NetTop Improved Assurance Configuration

Another critical component of the underlying host platform is the BIOS function that controls the initial boot-up process, and its ability to arrive at a secure initial state. Vulnerabilities in the BIOS have long been identified as the "Achilles' heel" of computer systems. Work presently underway to develop a robust, trusted BIOS should be incorporated into any high assurance NetTop system.

Failure Checking

Even a minimal NetTop configuration will be an extremely complex hardware and software system. It will not likely be amenable to the forms of failure analysis historically used for NSA high assurance systems. While it might seem that significant failures in a NetTop device would result in complete system shutdown, sensitive applications will require more rigorous assurance arguments. Lacking failure detection support in the workstation platform, an approach using a type of "dead man's switch" has been developed to limit failure effects by severing external NetTop communications.

In order to make an effective argument for the correct operation of a failure checking mechanism, hardware and software must be completely independent of the system being checked. A Dallas Semiconductor Tiny InterNet Interface (TINI) embeddable computer was networked to the in-line Network Encryptor machine, and was programmed to use a simple network "ping" to the VPN machine as a health check. If no response was received, the Internet connection was interrupted. A more robust health check could include a more complex set of tests to gain increased assurance that the NetTop device is working properly. The tests could include challenge/response exchanges with a Failure Detection Server in the protected enclave. A dead-man switch of this type may be suitable for a GOTS plug-in component for high assurance applications. The

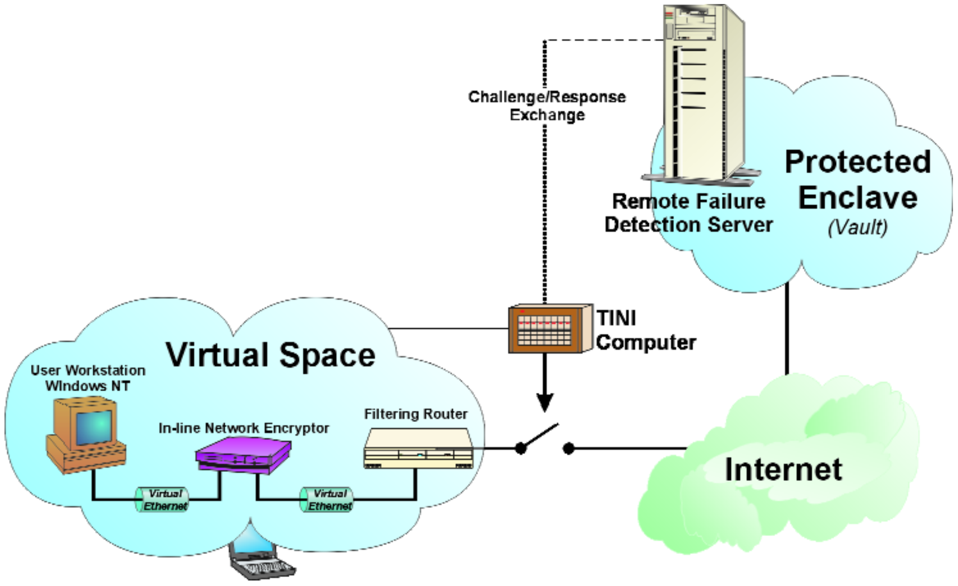

Challenge/Response Exchange
Remote Failure Detection Server
Protected Enclave
(Vault)
TINI Computer
User Workstation Windows NT
Virtual Space
In-line Network Encryptor
Filtering Router
Virtual Ethernet
Virtual Ethernet
Internet

Figure 7 - Dead-Man Switch Architecture

failure detection approach is shown in Figure 7.

Moving Data Safely

Many organizations require the ability to move information between networks of differing security levels. A common operation involves downgrading information from highly classified to lower classified systems, but increasingly, information is imported from the Internet into classified systems. In the first case, it is essential that classified information not be compromised, while in the second, a primary concern is the protection of the classified host from malicious content.

The VMware product includes a capability to copy and paste data between VMs via a clipboard. This feature does not include sufficient safeguards for use in a high assurance NetTop system. In order to provide a more trusted copy/paste function, a new capability, dubbed a "Regrader," was developed. This capability includes a protocol for performing the regrade operation, as well as a "Regrade Server" that provides a trusted network service. By making the regrade operation a centralized service, a number of advantages are gained. First, consistency in the regrade operation can be achieved. Second, it would be possible to develop and enforce a regrade policy that specified the conditions under which each user could perform regrade operations. The regrade operation could include "sanitization" functions to deter the transfer of covert or malicious content. Finally, an audit log could be maintained and monitored for suspicious activity. Figure 8 depicts the protocol exchange between the Regrade Server and two hosts of different security levels. A trusted user token is employed in a challenge/response exchange with the trusted server in order to safeguard against untrusted OS behavior.

Coalition Support

The paradigm of virtual machines creates abstractions of physical computers. Each VM is composed of a set of files that embody a hardware/software system. This set of files can be copied from one physical machine to another. Given the portability of VMs, there is no inherent reason why a VM, or set of VMs, could not be electronically transferred. It is possible for a NetTop device to become a member of a coalition by downloading an appropriately configured VM over a secured communications channel. The set of VMs in each coalition would constitute a VPN, and would not be able to communicate directly with VMs in other coalitions. Cross-coalition communication is performed using

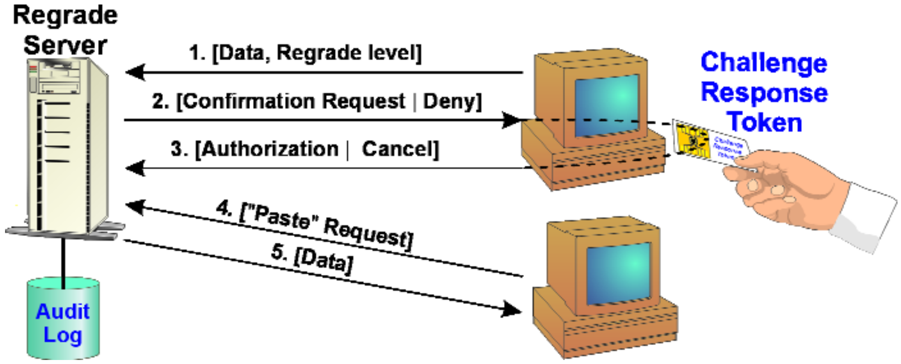


Figure 8 - Regrade Server Protocol

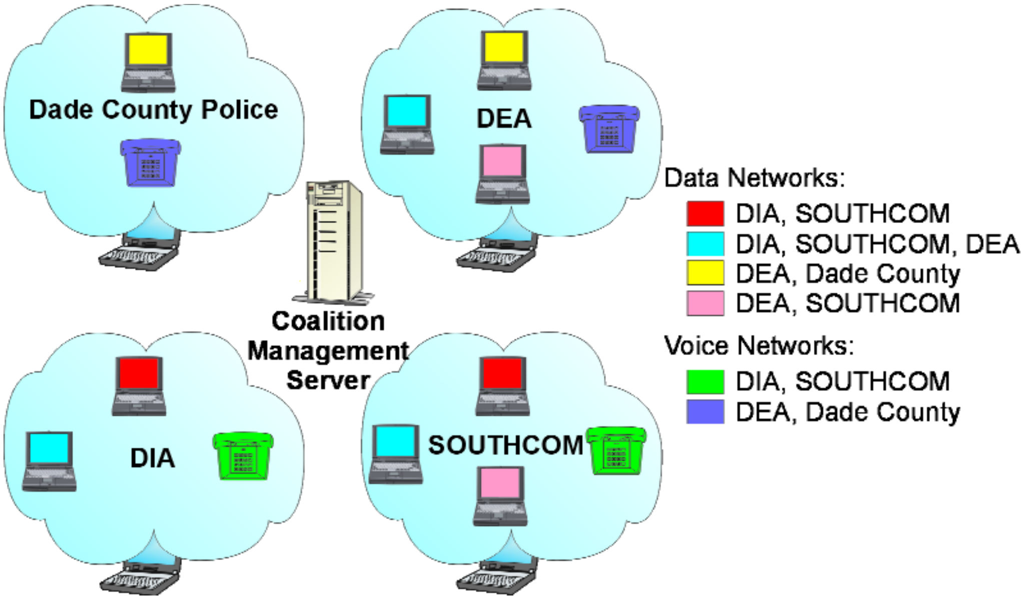


Figure 9 - NetTop Coalition Concept

a variation of the Regrade Server previously described. For some coalitions, it might be useful to distribute application specific VMs, such as a secure Voice-over-IP machine. A centralized Coalition Management Server could be used to manage the configuration and distribution of VMs to coalition members. The essence of NetTop's coalition support is its ability to distribute virtual systems electronically. Figure 9 displays a hypothetical situation in which four organizations participate in four data coalitions and two voice coalitions. A simple capability to demonstrate electronic distribution of VMs is under development.

Additional Capabilities

A number of useful capabilities are included in the prototypes that were not described in the NetTop overview. The entire file system on the hard disk is encrypted in order to protect against compromise if the machine is lost or stolen. The "International Patch" for Linux was installed, which provides software encryption capabilities and services under the control of the Trusted Linux host OS. The hard disk encryption is transparent to all VMs. Additionally, this disk encryption cannot be corrupted or bypassed by an VM. A process was developed that uses a floppy disk and a user entered PIN to "bootstrap" the decryption and loading of system files from the hard disk. During normal operation, all disk files, including temporary files, are stored encrypted on the hard disk.

The hardware virtualization provided by the VMM also provides a capability to alter the operation of the hard disks seen by each VM. In one mode, all changes made to a VM's hard disk are discarded when it is powered down. This may be useful in the operation of the IPSec and FR machines by preventing permanent changes to the system if a successful attack did occur. Any changes would be lost when the VM was restarted, which would force an adversary to repeat the attack.

Performance

Real-world performance determines any technology's acceptance. NetTop's architecture includes a lot of functionality in a single hardware platform, yet the performance is quite acceptable. The laptop computer used in the prototype includes a 500 MHz Pentium III processor and 384 MB of memory. The VMware VMM is surprisingly modest in its affect upon the performance of a VM, and only a slight degradation is noticed. As more VMs are introduced, more serious performance degradation is noticed, but can be minimized with additional memory. The 384-MB configuration of the NetTop prototype shown in Figure 4 was sufficient to support the Linux host and four guest VMs - two Windows NT machines for the end-user terminals and two Linux machines for the in-line Network Encryptor and Filtering Router. Overall, the performance of the NetTop prototype is quite satisfactory, and easily keeps pace with a high-speed, cable modem connection. Continuing enhancements in hardware performance will only improve its performance.

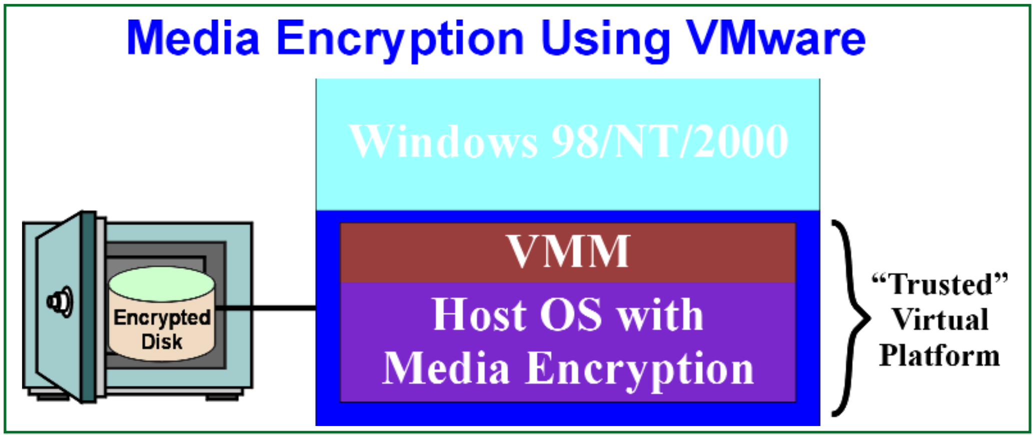
Future Development

The NetTop proof-of-concept has demonstrated an architecture that appears to have significant promise for information assurance applications. In its current form, however, it is unsuitable for widespread use and requires considerable refinement. Our research has uncovered a number of shortcomings in current technology that need to be addressed. Additionally, important topics still must be investigated. Areas requiring further development are:

- Identification & Authentication Architecture
- Biometric activation technique
- Key & certificate management
- Filtering Router management
- Un-spoofable labels for MSL windows
- Trusted VM switching mechanism
- Installation & configuration wizards
- IPSec modifications for NetTop protocols
- User friendly interfaces

The set of capabilities identified as NetTop extensions - Failure Detection Server, Regrade Server, and Coalition Management Server - suggests an expansion of the security services typically considered as part of a Security Management Infrastructure. The integration of these services with traditional key and certificate management services may deserve a separate investigation to develop a concept for a more comprehensive security infrastructure.

Development of the NetTop prototype is continuing. Some of the concepts previously described including a Regrade Server, thin-clients, and coalition support will be integrated as each is developed.


Media Encryption Using VMware

A very simple NetTop configuration with only one user Virtual Machine can provide a very useful feature - media encryption - which could not otherwise be done with a high-level of confidence. Since the host operating system does not run applications software, it is protected from virus attacks and other malicious software that might corrupt the user VM. With the media encryption function embedded in the host OS, all of the files on the hard disk can be encrypted transparently to the user OS. The user OS cannot bypass the cryptography that is protecting the media.

Conclusion

The Information Assurance Research Office has responded to the NSA Advisory Board's challenge with the NetTop proof-of-concept. The novel architecture builds upon COTS technology, fortifies it with GOTS components, and provides a combination with the potential to be securely used for sensitive applications. It also addresses other important concerns, and provides a framework for useful extensions. NetTop depends heavily upon the isolation capabilities provided by the Trusted Linux/VMM combination. The robustness of the approach still requires a comprehensive security evaluation.

Donald Simard is the Technical Director for the System and Network Attack Center and has been with the Agency since 1979. The majority of his work has been in the Information Systems Security Organization. He is a Master in the INFOSEC Technical Track and has a Masters Degree in Computer Science.

Robert Meushaw is Technical Director for the Information Assurance Research Office. He joined the Agency in 1973 with BS and MS degrees in Electrical Engineering. Mr. Meushaw had a long career in the Information Systems Security Organization prior to his current position. He is a Master in the Computer Systems Technical Track.