

NetTop Eight Years Later

Robert Meushaw and Don Simard

In the summer of 1999, NSA's most senior Advisory Board issued a report warning of a serious and growing problem in the protection of government's most sensitive information systems. The Board's concerns acknowledged the dramatic decline in information assurance that many professionals had observed over the previous decade. Surprisingly, this decline occurred in spite of major advances in computer security spurred by the establishment of the National Computer Security Center (NCSC) in 1981 expressly for the purpose of securing critical information systems. Numerous high-assurance computing platforms were produced as a result of the NCSC's efforts, but none seemed capable of coping with the impact of the decade's technological phenomenon—the Internet. The 90s produced an explosion of new networking systems and services, and the widespread availability of powerful and inexpensive commodity workstations powered by Microsoft's ubiquitous Windows operating system. Not even the national security community could resist the functionality and cost savings this technology delivered, despite numerous assessments of its negative impact on security. Commercial-off-the-shelf (COTS) information technology had established a permanent foothold within government.

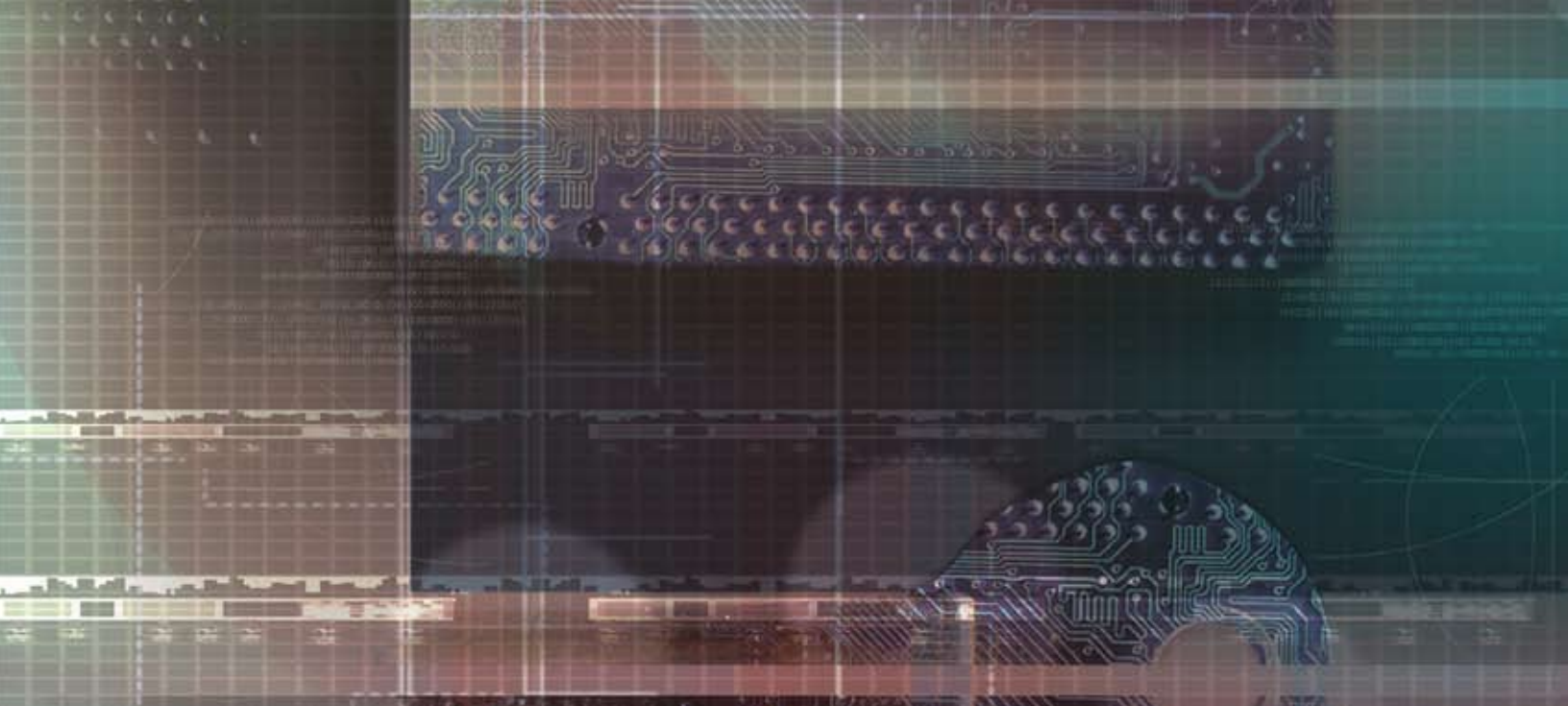
NSA's Information Assurance Directorate (IAD) responded to the growing use of commercial technology with a number of new initiatives. Some attempted to raise the level of security provided by commercial products, but the government market was far too small to have any real influence with successful commercial vendors. The much-publicized and valiant Multilevel Information System Security Initiative (MISSI) with its flagship Fortezza encryption card attempted to provide a high assurance overlay to bolster the security of commercial products, but it too lost the battle of cost, convenience, and interoperability in the desktop space. As the 90s drew to a close, NSA's approach to information assurance shifted to emphasize perimeter defense, intrusion monitoring, and risk management. This situation prompted NSA's Advisory Board to sound an alarm. The Board saw the government's most sensitive information systems being dominated by COTS technology incapable of providing the necessary levels of security, and a government market insufficient to influence vendors to provide the requisite protection. The Advisory Board called for a new strategy to be developed that could leverage the commercial technology that users wanted but still provide the higher levels of assurance they needed. The Board's report included a specific

challenge to NSA's Information Assurance Research Group to launch a new effort to deal with this problem. To ensure that their challenge was handled with appropriate urgency the Board insisted that a solution be developed within one year! The challenge was accepted, and the result was NetTop.

NetTop was originally described in the Fall 2000 issue of *Tech Trend Notes* (predecessor to *The Next Wave*). At that time the project had just started and we were developing many new ideas for potential applications of the technology. We optimistically thought that within three to five years we could get the technology into our customer's hands. Today, eight years have passed and NetTop has yet to achieve widespread use. So what happened? The editors of *The Next Wave* thought that a retrospective look at NetTop's history might be both interesting and informative. This article describes the evolution of our research and some of the novel approaches we attempted in order to deal with the perennial problem of technology transfer.

Early R&D

NetTop began as a research initiative responding to a challenge of NSA's Scientific Advisory Board. The intent of the project was to explore new concepts for security architectures. It was not envisioned



as the first stage of a new but traditional product development. Historically, NSA's product developments have mainly focused on link encryption solutions, many fielded in excess of 20 years but still capable of providing protection from cryptographic attacks even years after being removed from service. This approach to system security had worked well for decades, but it wasn't delivering the kinds of solutions needed to protect modern information systems against the new, active threats encountered in networking environments. A new model for Information Assurance (IA) solutions was being sought—one better suited to today's IT environment and capable of providing incremental security improvements over time.

The IA Research Group accepted the Advisory Board's challenge and established a senior-level tiger team to respond. To meet the one-year deadline, the group quickly focused its attention on some relatively well-understood technologies rather than defining a totally new research activity. Within several months we identified an approach using an interesting "technology cocktail" that looked very promising. The first component of the cocktail was a *refreshed* version of 1960s era virtual machine (VM) technology that had emerged from DARPA-sponsored research, and was

brought to market by a start-up company known as VMware. The second ingredient was an NSA prototype operating system—Security Enhanced Linux (SELinux)—that was gaining traction in the Open Source community. The combination of these technologies seemed to offer interesting possibilities for combining the COTS hardware and software that users wanted with the transparent security controls they needed.

Because of the unusual events that unfolded during the course of our work on NetTop, it became necessary for us to take our concept demonstration to a much more advanced stage of development than usual, and we found ourselves in the uncomfortable driver's seat of product developers. As we worked through the issues associated with developing NetTop for operational use, we had to answer a number of important questions:

"Can we do this?" – Will the technology work for the kind of applications that users want?

"Should we do this?" – Does the technology protect against expected attacks without introducing new and more serious problems?

"Will we do this?" – Can we deploy this new solution and sustain it in the field?

Our experiences as we attempted to answer these questions are the real story behind NetTop.

Can we do it?

After developing a crude first prototype of NetTop, most of our time was spent trying to determine if virtualized components were practical for use in systems that solved important user security problems. Although we encountered many technical challenges as we tried to integrate SELinux and VMware into a secure configuration, this portion of the project proved to be the shortest phase of the overall effort.



NetTop prototype

Does virtualization help to solve real problems?

One of the first uses for NetTop that we considered was as a Remote Access solution that would allow users to connect to a secure enclave remotely using a commercial laptop computer. Within several months we had a rudimentary prototype demonstrating this capability, and we soon realized that we should be able to do much more with system architectures using virtualized components. If we could efficiently support multiple virtual machines running concurrently on a single workstation, then numerous other types of solutions would be possible. The NetTop prototype we constructed turned out to be just one instance of a general architectural approach to building solutions that could be used to solve many different security problems.

Remote Access Solution Lessons Learned

Working with our first NetTop prototype helped us to distill a number of important characteristics and benefits of virtualization as an isolation mechanism.

▶ Isolating a security critical component like an IPsec encryptor in a separate container shielded from the behavior (or misbehavior) of the user's commodity operating system and applications was helpful in restricting the impact of software attacks. For example, an IPsec encryption stack

installed within a Windows OS can only be as trusted as Windows itself. But installing the same IPsec stack in its own container and linking it by a network connection to the Windows container provides an Inline Network Encryptor (INE) architecture that limits the avenues of attack to just the network interfaces. See Figures 1a and 1b.

▶ Providing multiple virtual machines for a user gave us an opportunity to create multiple single security level environments running simultaneously. This capability was sometimes confused with the traditional notion of Multi-level Security (MLS) in which a single environment protects information objects with multiple security levels. To help avoid this confusion we coined the term "Multiple Single Level" (MSL) to describe the capability that the NetTop architecture provided. See Figures 2a and 2b for a side-by-side comparison of MLS and MSL architectures. Using an MSL approach to architect a solution would involve using a collection of single security level VM's that could communicate with each other using network connections. This approach to designing solutions gave rise to the name NetTop—a **Network** on a **deskTop**. Each of the individual VMs would contain only data at one security level. Even security critical VMs such

as encryptors could be limited to processing data at one security level, thereby reducing their complexity compared to devices that manage data and keys at multiple security levels. Another approach that used the concept of isolated containers known as MILS (Multiple Independent Levels of Security) was promoted for use in embedded systems. While MILS technology provided very high assurance isolation, it didn't have NetTop's capability of hosting Windows or other legacy operating systems and applications, and so it wasn't as useful for typical user needs.

▶ Using partitions to separate information based upon integrity levels provided another capability that was useful in some applications. One such solution we developed—BoxTop—permitted the execution of suspicious, and potentially malicious, programs in a confined space and ensured that any harmful activity within that space could not spread further. We used one-way network connections to transfer content into the container, but no connection was provided for transferring data out of the container. This "virtual blast cage" could fall victim to an attack, but the damage was blocked from propagating further.

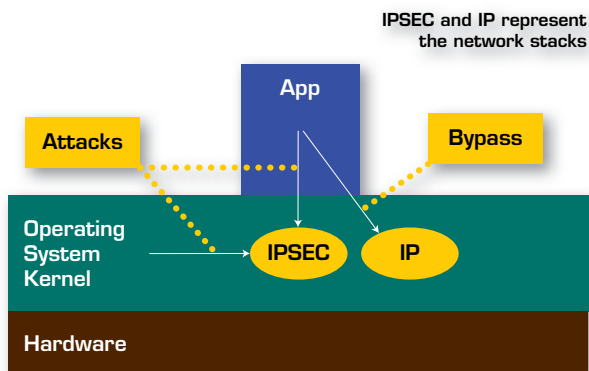


Figure 1a: No virtualization layer. Attacks against the IPSEC can come from an application or through the OS. An application can bypass the IPSEC and attack the IP directly.

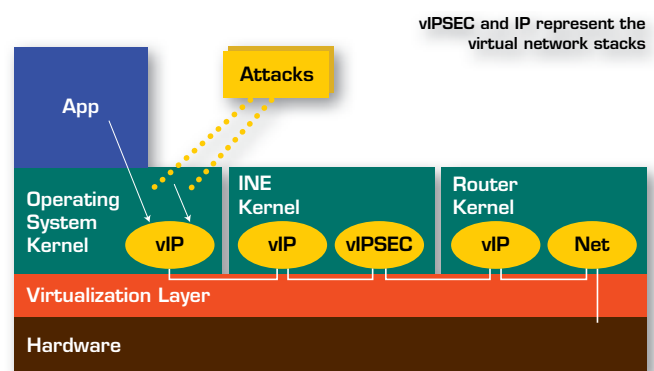


Figure 1b: With a virtualization layer. Attacks from the OS and application are confined.

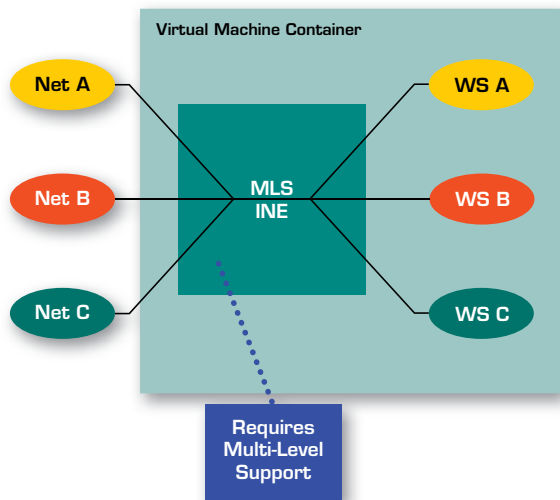


Figure 2a: Graphic of traditional Multi-level Security (MLS)

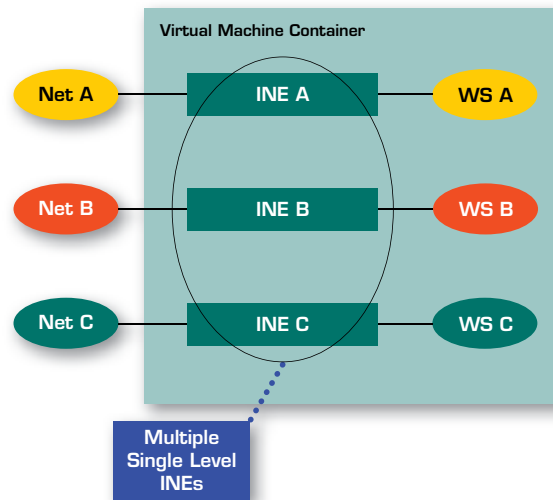


Figure 2b: Graphic of Multiple Single Level (MSL), a capability that the NetTop architecture provided

► The isolation provided by the use of separate virtual machines ensured that changes to system components that were not security critical would not impact security-critical components, and should reduce, if not eliminate, the need for lengthy re-evaluation of the overall system. This use of isolation improved NetTop’s agility by allowing it to quickly incorporate new commercial capabilities without disturbing security-critical components. We were able to quickly create versions of NetTop that used direct ethernet connections, modems, or wireless network adapters since no changes were required to the encryptor VM.

On July 13, 2000, two months earlier than requested, we met with the Advisory Board to describe the architecture and demonstrate the prototype we developed in response to their challenge. At the end of the briefing the Board surprised us with an unprecedented round of applause for what they saw as a creative and useful first step to dealing with security in COTS technology. Subsequent phases of the project would prove to be much more difficult.

Should we do it?

Study 1: Does NetTop introduce more problems than it solves?

We soon convinced ourselves that a variety of useful solutions could be designed using the NetTop architecture. The next important question that we had to answer was whether our approach would introduce more problems than it was solving. To answer this question we sponsored a workshop using some of NSA’s best security evaluators to assess our prototype. Using seven analysts over a ten-week period and with some limited input from VMware developers, we explored the ability of the core NetTop technologies—VMware running on a Linux host—to maintain isolation among virtual machines and to maintain isolation of the Linux host from the virtual machines.

The results of this first study were encouraging—no apparent show-stopping flaws were identified. The analysts were given full access to a VM and were able to write any program they wished in an attempt to crash another VM or the host OS. VMware workstation reliably withstood the attacks that were attempted and although a VMware virtual machine could be crashed, the host OS and other VMs were unaffected. Following these experiments, we expanded our relationship

with VMware through a Cooperative Research and Development Agreement (CRADA) to facilitate further NetTop development.

Study 2: What kinds of network attacks does NetTop prevent?

Our first NetTop study investigated the security robustness of a standalone workstation, but we still needed to address issues that might arise when network connections were allowed. So the next question we wanted to answer was whether there might be any unique remote attacks against a NetTop virtual machine solution that didn’t exist in an identical system using real machines. This was the focus of our next experiment.

In the summer of 2001 we were able to take advantage of a high profile NSA intern program established to develop network security experts. As the final project for the graduating class we devised an exercise to study network attacks against the NetTop virtual platform. The intern group was composed of fifteen network security specialists who worked over a period of twelve weeks and were led by one of NSA’s most talented and respected evaluators. Motivation in the group was high. They were eager to show that our solution was flawed. Some of the bolder analysts were confident that

they would uncover “holes big enough to drive a truck through.” The class project was scheduled to run through the end of September 2001.

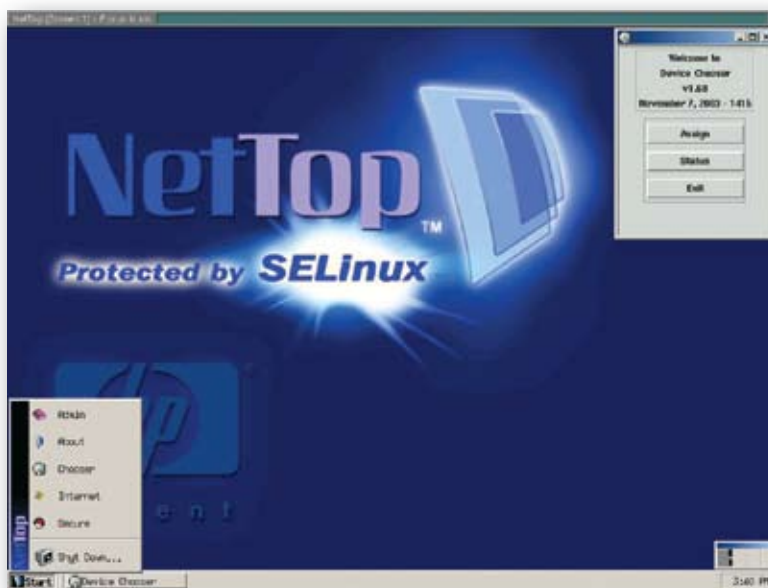
For this exercise we created a specific NetTop configuration that used two virtual machines running simultaneously, with each VM attached to a different network—in other words we created a “virtual KVM switch.” The user interface experience was one familiar to VMware users—two different desktops in two separate windows. We used SELinux as the host OS with a security policy crafted to provide maximum protection for the host. The sole function of the SELinux host was to provide an execution environment for the virtual machines. No user accounts or user applications were allowed on SELinux. It was a very tightly controlled configuration. In fact it was so tightly controlled that the interns requested a relaxation in the SELinux policy in order to allow an initial toehold for their attacks.

The group identified a number of areas that could be improved and they pointed out some lifecycle issues that should be considered in future deployments. But in the end this study reached conclusions very similar to the first, and no show-stopping problems were found.

Will we do it?

From the outset our goal for NetTop was as much about developing new technology transfer approaches as it was about developing new technology. The motivation behind the NSA Advisory Board’s challenge was that government needed more innovative approaches for leveraging commercial technology so that it could be used for sensitive applications. Government-unique IT developments (government off-the-shelf or GOTS) were far too costly to create and maintain, and frequently lacked capability compared with COTS offerings. It was

clear that users were simply not willing to pay a premium for higher assurance. Our previous experiences with MISSI and Fortezza were lingering reminders of this. It seemed to us that the most direct approach for dealing with this problem was to develop technology that was useful for government applications but that also had broad appeal outside of government. We believe that if we could stimulate the development of a large commercial market for this technology, the government could benefit from the cost advantages of large-scale COTS production. In effect we were conducting research in market development as much as in new security technology.



NetTop and SELinux

We used a relatively new NSA program—the Domestic Technology Transfer Program (DTTP)—to help us with our attempts at market development. This program had been established in response to US Code Title 15, Chapter 63, Section 3710, “Utilization of Federal technology,” to promote the transfer of government sponsored research to the public sector. The DTTP provided experts to assist us in numerous areas related to tech transfer including identifying candidate technologies, technology valuation, acquisition of ownership rights, finding transfer partners, establishing partnering agreements, negotiating transfer agreements, and overseeing relationships.

One of our first steps after demonstrating our prototype in March 2001 was to file a patent application to gain control of the intellectual property (IP) embodied in NetTop. In a somewhat unusual move for NSA, we also decided to seek a trademark for the name “NetTop,” since it had gained a fair amount of recognition and therefore seemed useful to control. We wanted to avoid the unfortunate situation encountered in the MISSI program when their flagship Fortezza token had to change its name from Tessera because of a trademark-filing oversight. The NetTop trademark proved to be very useful in later phases of the marketing program. Having protected NetTop’s IP and name, we began a search for industry partners capable of commercializing it.

While our main effort was to transfer our technology to a commercial partner, we knew that an NSA support group for NetTop was needed outside of the research organization. We believed that NetTop’s long-term success and its commercial development strategy needed a program office within the IAD—NSA’s arm responsible for developing security solutions. Unfortunately there wasn’t any pull from the IAD for NetTop or its component technologies—SELinux and VMware. NetTop was seen as lower assurance than the solutions that the IAD normally produced or endorsed. From our point of view, NetTop offered an approach that could deliver “high impact” to the assurance of customer missions rather than just “high assurance.” Our belief was that it provided a mix of functionality and value that users would embrace, rather than the high assurance products that were often developed but not widely used. We also believed that NetTop provided much better assurance than the COTS alternatives that customers were adopting. Furthermore we saw a migration

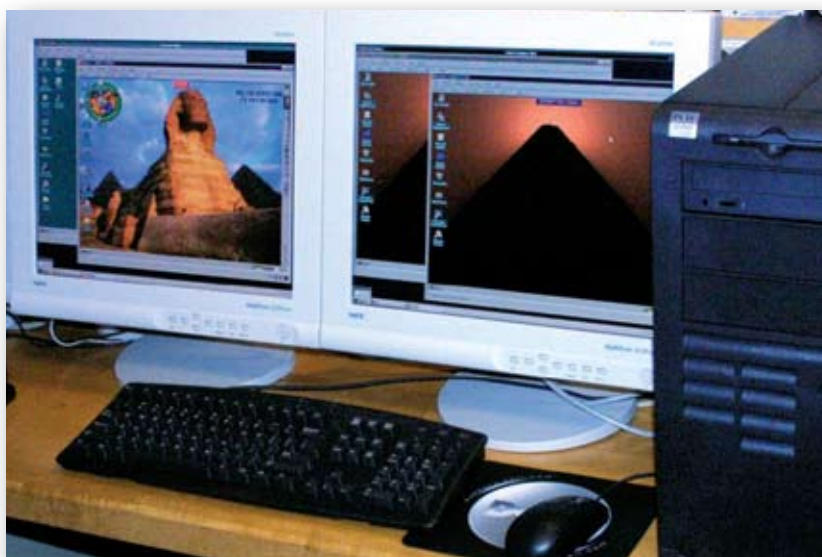
path for NetTop to even higher assurance solutions in the future. NSA's Advisory Board seemed to agree, and in a July 2001 meeting they recommended that the IAD establish a program office to manage the development of NetTop solutions.

The IAD approached the establishment of a NetTop program office very cautiously. A number of studies were undertaken to suggest a product roadmap, an assurance improvement roadmap, a business plan, and an assessment of NetTop's Total Cost of Ownership. The outline that was developed for productizing NetTop focused on the simple virtual-KVM configuration that was built for our ongoing security evaluation, with the added restriction that only adjacent security levels be permitted (e.g. Top Secret to Secret) and that cross domain data movement be prohibited. A management meeting to decide on the way forward was held on September 10, 2001—but no decision could be reached. Ironically, the terrorist attacks of the following day—September 11, 2001—and the US military response did determine the course of the program.

The US Central Command (CENTCOM), headquartered in Tampa, Florida, led the US military response to the terrorist attacks along with a large collection of coalition partners. IT support for this immense operation was a daunting task, and the crush of equipment required to access numerous coalition networks strained available space and power. On a visit to CENTCOM shortly after 9/11 an IAD representative noted this problem and wondered if NetTop might offer relief as a desktop reduction solution. This idea was suggested to IAD management as a unique opportunity for technology insertion. The intern class that was evaluating NetTop was still working when the idea of using it at CENTCOM surfaced. Because of their recent security evaluation

experience, the class was viewed as a useful sounding board, so they were polled regarding NetTop's suitability for use at CENTCOM. The consensus was that NetTop was sufficient for separating adjacent security levels (TS and S for example), but the group was reluctant to give an unqualified recommendation for its use to simultaneously access Unclassified networks. This endorsement was a significant milestone for the project, NetTop had been able to transform a highly motivated group of skeptics into supporters, albeit cautious ones.

IAD management agreed that NetTop could improve CENTCOM's operations, and that it should be quickly retooled



CenTop Workstation

for use in an operational environment. A NetTop Program Manager (PM) was named within the IAD's product development organization, but because of the urgency of the CENTCOM requirement, the research group was given responsibility for developing and fielding the production equipment.

The NetTop prototype needed extensive hardening and refinement to make it suitable for use by typical military operators who weren't hard-core system developers. To accomplish this, NetTop received a complete face-lift to remove the most visible signs of its Linux heritage. The user interface for CenTop—CENTCOM's custom NetTop implementation—was

redesigned from the top down to give it the familiar look and feel of a standard Windows workstation.

Other design changes targeted to CENTCOM's operational needs included an ability to access six networks simultaneously, dual monitor support for more desktop workspace, and the ability to run CENTCOM's standard Windows software load in each VM.

By the end of December 2001 a small team had been assembled to help the NetTop PM manage the myriad activities required to advance NetTop's development. Most important was the transition of NetTop to CENTCOM, which required the initiation of a security evaluation and generation

of the large body of documentation required by the accreditation process. Other important activities included establishing a small NSA NetTop pilot, collecting feedback on user and administrator acceptability, and providing support to NetTop developers.

The eventual transition of NetTop to CENTCOM was well intentioned but, unfortunately, not well executed. While the technology was well received by users,

the various support groups that had to administer it were not equally enthusiastic. A number of operational difficulties were encountered, and while most weren't due to design problems they nevertheless contributed to an overall negative initial impression of the technology. One of our major oversights was not having 24/7 NetTop support available from the outset. This problem was eventually corrected, but the delay proved to be a costly misstep in NetTop's first high-profile deployment. In retrospect, we should have ensured that NetTop had a high-level CENTCOM advocate as well as buy-in from the IT support groups.

After the initial intensity of the coalition military effort subsided, the

urgency to field NetTop at CENTCOM diminished as well, and with it the pace of the evaluation activities. Even with the urging of the NetTop project management office, it took over 18 months before formal decisions were reached about appropriate uses for the technology. Based upon a growing body of technical evidence, including the results of the two earlier evaluations and another evaluation on the CENTCOM-specific NetTop solution, the IAD Director finally approved NetTop for classified applications, but its use was limited to applications needing to separate Top Secret and Secret networks. Having taken over three and a half years to reach this point was disappointing, but the research team was never the less euphoric at reaching this important milestone. Unfortunately the feeling was short lived as we came to the realization that the use of NetTop throughout the Intelligence Community (IC) would require yet another extensive, bureaucratic accreditation process – DCID 6/3. This meant we had to socialize NetTop’s concepts

to yet another group of accreditors and Designated Approving Authorities (DAAs) that had never before seen this type of solution. Furthermore, the DCID 6/3 evaluation criteria used by the DAAs were not designed to address solutions like NetTop that had multiple operating systems running con-currently. DAAs rarely decide issues concerning operational use of security solutions without involving their peers, since individual decisions often create shared security risk across the community. So we once again found ourselves having to educate numerous decision makers about why NetTop should be approved for operational use. Eventually our efforts succeeded, and in the following five years NetTop began to

find use in various deployments. Although painfully slow at the outset, NetTop has continued to gain acceptance as a security solution within the IC and the DoD.

Finding Tech Transfer Partners

Shortly after our decision to pursue a tech transfer path for NetTop through the licensing of intellectual property, the research team initiated a series of meetings with potential commercial partners. The most promising partner initially was the Federal Division of Compaq Computers. Compaq management saw potential in NetTop to help them build a market in

a competitive market would be even better for the government. After two more years of discussions with other potential partners we negotiated a second NetTop license with Trusted Computer Solutions (TCS). TCS was much smaller than HP but very well established in the government market for security products, and they were highly experienced at working with the security accreditation process. TCS’s strengths seemed like an excellent complement to HP’s for developing a significant market for NetTop.

Several months after licensing NetTop, HP was able to generate some interest in the technology from their government customers, and they have continued to steadily grow their sales. Ironically, NSA did not become a strong customer because IT support at NSA had been outsourced to an industry consortium, and NetTop’s approach wasn’t consistent with the terms they had bid in their contract. TCS also began to see some interest in their NetTop offering shortly after they licensed the technology. Unfortunately we

didn’t see the dramatic uptake of the technology that we expected. After several years reflecting on this situation we began to understand why our expectations weren’t being met. Both of our NetTop partners drew their customers from the high assurance DoD and IC market space rather than the broader commercial market, and their revenues were heavily dependent upon selling services rather than products. There was little incentive for them to drive product costs down since they weren’t anticipating a mass consumer market for NetTop. In the high assurance government market, NetTop sales may grow but probably only at the pace of IT infrastructures replacement; so while we may eventually see increased deployments,



HP and TCS NetTop marketing material

security-related IT. Our discussions with Compaq were very positive, but they were soon interrupted because of the prospects of a merger with Hewlett-Packard. After completion of the merger in September 2001, discussions resumed with the new Federal Division of HP. But it was not until November 2002, almost two years after the start of discussions, that a NetTop license was finally negotiated. We viewed this milestone as a tremendous accomplishment and were certain that we would soon see a large commercial market for NetTop that the government could leverage. We were only partially correct.

While we worked with HP to help them refine NetTop, we continued to seek other commercial partners, since we believed that

they are likely to be over a much longer period of time than we expected. It's also unlikely that we will see costs drop as significantly as we had hoped.

Checking Our Projections

In our Fall 2000 NetTop article, "NetTop—A Network on Your Desktop," we speculated about the potential of virtualized architectures to deliver many more capabilities than the remote access solution we started with. Two of the solutions we described included a multi-domain access system and a coalition support system that provided dynamic collaboration environments. In the years since our original prototype, we went on to develop systems very similar to those we described. The workstation that we developed for CENTCOM, in fact, implemented our concept of a multi-domain access solution. We later developed a proof-of-concept system called the Intelligent Infrastructure Demonstration (IID) that showed how dynamic, private collaboration environments could be created rapidly to support mission needs for information sharing. In the following years, we created several other security solutions that we had never imagined, but which helped solve some of NSA's unique IT problems. These solutions further proved the adaptability and flexibility of NetTop's architecture.

Collaboration on Demand – Intelligent Infrastructure Demonstration

The original NetTop prototype was developed with a very tightly controlled configuration and lacked the flexibility to respond quickly to changing user needs. In short, it had the same limitations as the physical systems that it replaced. But in our *Tech Trend Notes* article we suggested the possibility of using virtualization technology to rapidly create new systems of various types and distribute them electronically wherever they might be needed. In 2003 we developed a demonstration of this concept in the Intelligent Infrastructure Demonstration (IID) system, shown in Figure 3. This system used a centralized server that could provision and deploy vir-

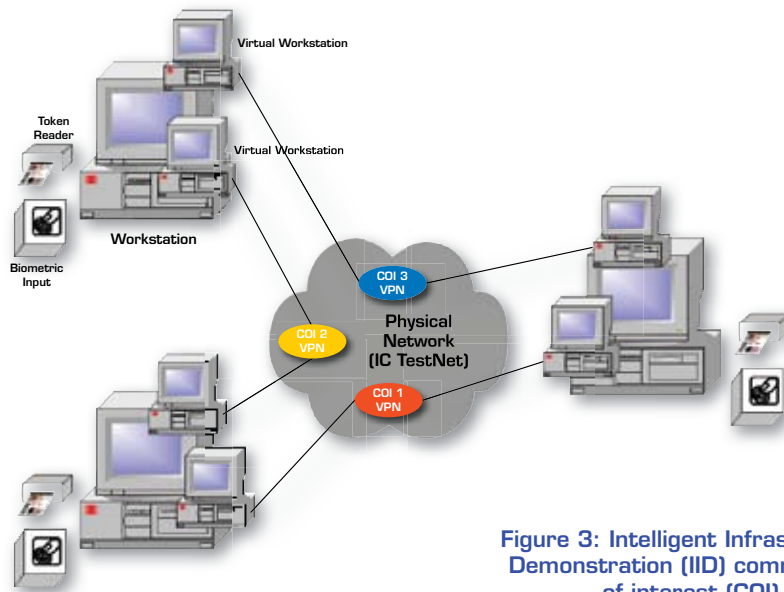


Figure 3: Intelligent Infrastructure Demonstration (IID) communities of interest (COI)

tual components including workstations, encryptors, firewalls, servers, etc., and then interconnect them to form private, collaborative workgroups or communities-of-interest (COI).

Our goals for the IID were to demonstrate how secure, collaborative environments could be set up easily and quickly to support the type of multi-party activities being performed at CENTCOM and other government organizations supporting the war effort. We wanted a capability that would enable the average analyst to set up a COI within minutes, tailor it to the needs of a particular group, and require no administrative support. As a model for IID

operation we used the Internet USENET system, which allowed individuals to easily create news groups for information exchange.

In our prototype each IID workstation was a NetTop that implemented a multi-factor (e.g. fingerprint, password, token, etc.) user authentication system and a special virtual machine dedicated to COI establishment and management functions. If a new COI were needed, a user could specify the members of the COI, the COI security level, the operating system to be used, and the set of application programs to be included. The management service would establish network servers to sup-



BoxTop interface

port the COI and invitations would be sent to the participants to join the COI. When a user accepted the invitation his workstation would receive software to configure itself to participate in the COI. IID users could participate in multiple COIs simultaneously and move easily among them via window selection.

Malware Protection: BoxTop

A different problem came to the NetTop research team from analysts who dealt regularly with documents, emails, and multimedia files that might contain malicious code such as viruses, worms, or other malware. Their management's security policy wisely required them to move any potentially dangerous content to a standalone system in order to ensure the integrity of enterprise operations. Unfortunately, the inconvenience of transferring data and the time-consuming cleanup process following an infection made the analysts' jobs unworkable. To deal with this problem we developed a NetTop spin-off called BoxTop that could safely and easily handle malicious content.

BoxTop used two virtual machines—one to replace the analyst's normal workstation and a second that operated as a sacrificial quarantine zone for processing malicious data. Analysts used a simple one-way data pump to move files into the quarantine zone and a special printing mechanism that allowed information to be exported safely for reports. To further improve analyst efficiency, we provided a mechanism to restore the quarantine zone to a sanitized state with the push of a button. SELinux provided us with an extensive set of security controls that we used throughout BoxTop's design to guarantee that it operated safely.

Protecting the Enterprise: ClearRealm

Following our work on BoxTop we discovered another enterprise IT problem that required a quick and innovative security solution. Unlike the case with BoxTop, where we were dealing with malicious data, this problem involved the use of enterprise software whose pedigree

was questionable. The normal software review and approval process was far too slow to meet mission needs, so managers were considering just installing the software and accepting the risk. We felt that we could leverage the flexibility of NetTop's architecture to quickly develop a solution that would allow the needed software to be used safely. In our ClearRealm design we encapsulated the questionable software as a web service and sandwiched it between two virtual firewalls to protect the integrity of the operational network. The firewalls were configured to ensure that the web service could not access the operational network and that it responded appropriately to user queries. ClearRealm proved to be very successful at meeting an urgent operational need.

ClarifyMind: Wireless NetTop

One of the significant benefits of NetTop's architecture is that it allows communication interfaces to be decoupled and isolated from components that provide security functionality such as firewalls, guards, encryptors, etc. Changes in network interfaces can then be made simply since they do not involve changes to security-critical code. We used this architectural approach in our original remote access solution to switch it between ethernet and modem connections, and we used it several years later in a wireless mobile solution called ClarifyMind. The prohibitive cost of new, wired connections to the desktop had denied Internet access to many analysts, so we proposed using NetTop to provide trusted wireless connections instead. To replace the security and access control of a wired connection we proposed using encryption of the wireless link. ClarifyMind's architecture combined a COTS laptop, an 802.11x card, MobileIP functionality, and an IP encryptor VM to deliver cost effective Internet access for analysts with the added benefit of allowing them to roam wirelessly. NetTop's architecture allowed us to isolate and protect the security-critical IP encryptor from other COTS components, and to ensure that all network traffic passed through the encryptor.

Application Partitioning

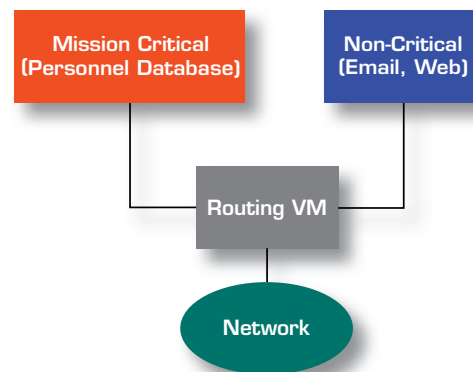


Figure 4: Using NetTop to isolate mission critical programs

Other Interesting Applications Isolating Mission Critical Software

During the course of our work we met with many different users to try to understand their operational IT needs, and we spotted several additional usage scenarios for NetTop architectures that hadn't originally occurred to us. One scenario involved a need to protect the integrity of mission critical applications from the potential misbehavior of non-critical Internet application programs. The prototype solution we developed used one virtual machine to run important mission applications (in our case a program to track troop deployment) and a separate virtual machine to run non-critical programs such as web browsers. By separating applications in this way we

Legacy Migration

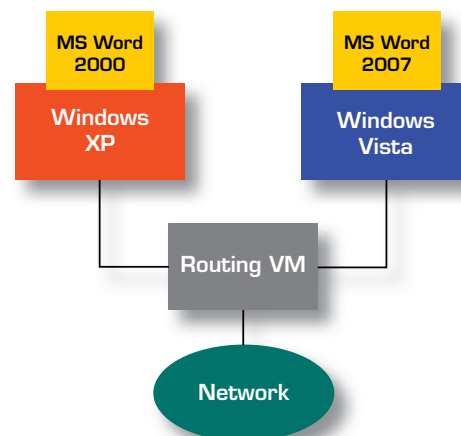


Figure 5: Using NetTop for incremental upgrade of new applications

showed that we could enhance mission integrity without losing desirable functionality. (See Figure 4).

Dealing with Software Migration

A second IT problem we discovered involved delays in deployment of current software versions across an enterprise. Users were often frustrated that they had to continue using outdated program versions until their entire suite of programs was updated to the latest operating system. This problem seemed like an ideal application for a NetTop solution that could provide multiple OS versions running simultaneously. This approach would permit applications to migrate individually and give users immediate access to the latest software versions. (See Figure 5).

Criticisms and Concerns

A healthy dose of criticism is not uncommon with any new technology, and it is par for the course with new security technology. But NetTop attracted a particularly broad set of vocal critics inside and outside of government. In part we believe this was because it represented a fairly radical paradigm change in its technical approach and also in its strategic approach to delivering security solutions via commercial partnerships.

The changes represented by NetTop were particularly uncomfortable for the IA community's traditional culture. NetTop attempted to strike a balance between the low assurance COTS technology being widely adopted by users and the very high assurance security solutions traditionally developed by government. It should not be surprising that neither community was totally satisfied with the result—but we believe that NetTop delivers a useful and credible blend of functionality and security.

Does NetTop Lower the Bar for Security?

One of the first criticisms of NetTop concerned its use of Linux as the host operating system. Linux was selected (actually SELinux) because we were able to customize it and rebuild the kernel to

provide tailored protection for the host OS. We were also looking ahead to the protection that SELinux' mandatory access controls could provide. To deal with potential vulnerabilities in Linux we used a number of design principles to minimize its risk of being exploited. First, we treated SELinux as an embedded OS and prohibited the use of any native user applications. VMware was the only application permitted. Our next step in reducing NetTop's attack surface, was to configure the system to make the SELinux host unreachable from any network connection. Since the time of the original NetTop evaluations SELinux has earned the same certification level (Common Criteria EAL 4+ LSPP, CAPP, and RBAC) as most of the host operating systems used in approved cross-domain solutions.

The environments originally intended for NetTop deployment only allowed access to users having the highest level of clearance of all connected networks in order to help deal with physical attacks. NetTop was often used in sensitive compartmented information facilities (SCIF) where all personnel were cleared to the highest level. Thus the environments intended for NetTop use were considered low risk.

Despite concerns expressed over the years about NetTop's security, it has held up well so far against sponsored evaluations as well as attempts to exploit weaknesses found in VMware's virtualization software. The combination of SELinux' mandatory access controls, VMware's isolation capabilities, and NetTop's tightly controlled architecture have proven effective at blocking attacks. While this is no guarantee that future problems won't emerge, continuing reviews by government analysts help to ensure that serious user problems are avoided.

Does NetTop Diminish the Market for High Assurance Technology?

In 1999 at the start of the NetTop project, users seeking trusted operating systems with a robust set of applications software faced a bleak situation. Those systems that offered the most functionality,

such as Microsoft Windows, fell short in security, and the several systems that offered very high assurance were lacking in functionality and interoperability. The NSA Advisory Board recognized that NSA's arguments for using the highest assurance technologies had long since ceased to be effective in the face of the COTS revolution, and users had opted for functionality over security. The Board was seeking a way to accommodate users' desire for fully COTS platforms while providing adequate assurance for sensitive applications, and they saw in NetTop a path for re-establishing a market for more secure products.

Prior to our work on NetTop, others had suggested a number of technical approaches to marry Microsoft applications with high assurance operating systems such as Trusted Solaris, but none of these products delivered acceptable performance and usability. Within NSA a high-assurance, thin-client architecture was developed as one possible way to give users a multiple security level capability, but it too had similar performance and usability problems. NetTop's architecture provided users with good performance from their Microsoft applications while at the same time keeping them isolated and protected in virtual containers. By interconnecting single-security-level containers, we could create solutions tailored to meet different users' needs.

We also saw in the NetTop architecture the potential to increase assurance over time by improving the security of its component parts. One way to increase assurance was by improving the host OS and virtualization environment that comprised NetTop's isolation infrastructure. A second way was to improve the assurance of individual virtual components. This second approach seemed to be particularly useful for creating specialized components that were hidden from users such as routers, firewalls, and encryptors. We had discussions with several high assurance OS vendors about migrating the NetTop architecture to their products, but concerns about the impact to their own products proved too difficult to overcome.

Does Virtualization Create a Security Problem?

One of the problems NetTop faced shortly after it was prototyped was that neither users nor system accreditors had a good understanding of the virtualization technology it was using. Although virtualization technology was originally developed in the 1960s, primarily for use with large-scale computers, its re-emergence on desktop computers in the late 1990s made it a novelty once again. Lack of understanding led to suspicion and fear about problems that might be lurking, but over a period of several years the issues associated with virtualization became better understood within NSA's IA community. Designing NetTop with security as a primary concern taught all of us a great deal about how to use virtualization prudently.

The commercial IT benefits of virtualization have been amply demonstrated by the dramatic growth of VMware over the past several years. But as the technology has become mainstream, the same security concerns that we encountered years ago re-emerged—this time from security professionals outside of government. Some of the recent security concerns with virtualization have been used as justification for dismissing NetTop's ability to provide robust protection. What many critics fail to appreciate is that most powerful tools can be used wisely or blindly with respect to security. We believe that NetTop's design offers a good example of how to use virtualization wisely.

Could We Do It Again?

The circumstances surrounding the development of NetTop were unprecedented for a research project. NSA's most senior Advisory Board identified a major security challenge and four of the Agency's most senior IA researchers, with over 80 years combined experience, were called upon to craft a solution. They, in turn, leveraged two of NSA's premier analyst development programs to perform in-depth security evaluations. The terrorist attacks of 9/11 were the catalyst that created a high priority military customer

and a committed NSA program to deliver an operational system from a research prototype. Over the course of several years, these events led us to some unique opportunities and to some useful insights into the business of research.

One of the unexpected benefits of our NetTop work was that it generated interest in partnering with research groups from a number of prominent IT companies. They sought to use our security expertise in operating systems and virtualization as a way to help them with their own technology developments. We saw an opportunity to use cooperative research as a way to gain significant leverage from our limited resources. We also saw potential in using cooperative research as a general technique for raising the bar in the assurance of commercial technologies. In effect we were developing a new COTS Security strategy based upon IA research collaboration.

A second benefit we derived from our work on NetTop and its spin-offs was that it served as a breeding ground for new areas of research. One interesting example was our early investigation of integrity checking for NetTop. This activity eventually blossomed into an important new area known as Measurement & Attestation, which deals with assured techniques for measuring the integrity of a computing platform and conveying this information to an enterprise health authority. This work could have future widespread use in the management of enterprise security, as well as more general application in developing trust among systems connected across cyberspace.

NetTop's developers had high expectations that the product's COTS-based blend of security, functionality, and flexibility would quickly generate a large market in public and private organizations that valued information assurance—unfortunately this didn't happen, and has been a major disappointment. What we came to realize was that sometimes technology changes are so dramatic that they require changes in organizational culture in order to succeed, and that

cultural changes often require a very long period of time.

Unfortunately for us, the cultural changes associated with NetTop involved changing not just one culture but two. The first was the crypto-centric, high-assurance product culture that was responsible NSA's long-standing reputation in security. NetTop used technologies unfamiliar and unproven to this culture, so they were considered unacceptable. NetTop was also built from COTS components incapable of delivering the assurance levels of GOTS products. It took years of experience with NetTop to build confidence to the point where it was accepted, at least for some applications.

The second culture that NetTop had to deal with was in the IAD's business community. In many ways this business culture was more difficult to influence than the high-assurance product culture. The bedrock of the business culture was the traditional, large-scale, FAR (Federal Acquisition Regulation) contract typically used for developing security products for customers in the national security community. Getting technologies like NetTop to customers involved a different approach, one similar to what industry would use. The new approach required aggressive practices in the creation and control of intellectual property, in marketing, and in developing and managing partnering relationships. We found little appreciation within IAD's business culture for the value of patents, trademarks, licenses, or open source developments because the use of these techniques were not deep-seated in the government business psyche. Contending with the business culture issues associated with NetTop required a major effort on our part, and added further delay to transfer of the technology. While we were somewhat successful in handling NetTop's unique business issues, to the IAD's business community it remains somewhat of an aberration rather than a useful, alternative business strategy.

We learned from experience that there is often a critical relationship between IA


technology and IT infrastructure, and that if a security technology isn't friendly to both users and to the infrastructure in which it operates, it just won't be accepted. We learned some hard lessons about this in our first NetTop deployment at CENTCOM. One unfortunate lesson occurred when one of the Windows VMs encountered the infamous Microsoft Windows "blue screen of death." The veteran operator reacted instinctively by hitting the machine's reset button. Unfortunately, this rebooted the entire set of virtual machines that were running and created a messy cleanup situation. We should have anticipated this would happen and ensured that only the crashed VM was rebooted. Other infrastructure management issues such as centralized auditing and remote platform configuration were also handled poorly in the original NetTop deployment. While these issues and many more have been addressed over time in improvements made to commercial NetTop products, they resulted setbacks for NetTop early in its development.

But—Would We Do It Again?

NetTop has not yet found widespread use outside of government, and this is a disappointment because we believed it would have many commercial uses. More importantly we hoped that commercialization would drive down the cost of the technology for government use, but this hasn't happened either. It isn't clear if a commercial market failed to materialize because of lack of user interest or because of inadequate marketing. Today NetTop is only available from vendors that focus on technology services for government rather than equipment sales. It remains to be seen if this will change in the future.

Although it would be impossible to recreate the extraordinary circumstances surrounding our work on NetTop, we have thought about whether we would undertake a similar effort in the future if we knew it would have a similar outcome. In short the answer is yes. The potential to have a major impact on customer mission assurance would still make such an effort

worth our investment. Through our work on NetTop we gained valuable expertise in an important, new technology area that allowed us to significantly advance NSA's acceptance of the technology and introduce new business strategies for product development. Another important consequence of our work was the ability to attract major industrial partners in collaborative research. These relationships have been very helpful in our research and particularly in developing next generation versions of NetTop through NSA's High Assurance Platform (HAP) project and our Secure Virtual Platform (SVP) research program.

Several thousands of NetTops have been fielded across elements of the IC and are being used operationally every day. Encouragingly, we have recently seen indications that NSA's own infrastructure upgrade initiatives are considering large-scale deployment of NetTop technology. While eight years is a long time to wait for this development, it is gratifying that our perseverance may finally be rewarded. 

About the Authors

Robert Meushaw is the former Technical Director of NSA's Information Assurance Research Laboratory (NIARL). He retired from NSA in 2005 after 33 years of service, including over a decade of work in IA research. Mr. Meushaw's career at NSA also included significant stints in both the Product Development Group and the Security Evaluation Group of the Information Assurance Directorate. One of his primary areas of focus has been the development of new strategies to transfer NSA-developed security research to the commercial sector in order to meet the needs of the Department of Defense and Intelligence Community for cost-effective, COTS security solutions. Mr. Meushaw is co-inventor of NSA's NetTop technology which is available commercially from Hewlett Packard and Trusted Computer Solutions. In addition to his technical responsibilities, he served for six years as Technical Editor of NSA's Tech Trend Notes and Next Wave publications. Mr. Meushaw holds degrees in Electrical

Engineering from Princeton University and The Johns Hopkins University.

Don Simard is a Technical Director in the NSA Commercial Solutions Center and has been with NSA since 1979. Most of his years were in the Information Assurance Directorate as a security evaluator. Mr. Simard has spent time in the National Information Assurance Research Lab and was one of the Co-Inventors of NetTop. He is a Master in the INFOSEC Technical Trace and holds a Masters Degree in Computer Science.