IAnewsletter

The Newsletter for Information Assurance Technology Professionals

Volume 6 Number 2 • Summer 2003

The Peter Kiewit Institute (PKI)

also inside—

contents

feature

IA initiatives

in every issue

About IATAC & the *IAnewsletter*—

IAnewsletter is published quarterly by the Information Assurance Technology Analysis Center (IATAC). IATAC is a DoD sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC), Defense Information Systems Agency (DISA).

Inquiries about IATAC capabilities, products, and services may be addressed to—

IATAC Director:	Robert J. Lamb
Deputy Director:	Abraham T. Usher
Inquiry Services:	Peggy O'Connor
Technical Analysts:	April Perera
	Jim Peña
Business Analyst	Brad Soules

IAnewsletter Staff—

Creative Director:	Christina P. McNemar
Art Director:	Ahnie Senft
Designers:	Maria Candelaria
	Holly Shipley

IAnewsletter Article Submissions

To submit your articles, notices, programs, or ideas for future issues, please visit http://iac.dtic.mil/iatac/news_events/author_submission.htm and download an "Author's packet."

IAnewsletter Address Changes/Additions/Deletions

To change, add, or delete your mailing or E-mail address (soft-copy receipt), please contact us at—

IATAC
Attn: Peggy O'Connor
3190 Fairview Park Drive
Falls Church, VA 22042

Phone: 703/289-5454
Fax: 703/289-5467

E-mail: iatac@dtic.mil
URL: http://iac.dtic.mil/iatac

Deadlines for future Issues—

Fall 2003	September 12, 2003
Cover design:	Holly Shipley
Newsletter design:	Ahnie Senft

Distribution Statement A:

Approved for public release; distribution is unlimited.

IATAC Chat

Robert J. Lamb, IATAC Director

The focus of this edition of the IAnewsletter *is education. Last quarter, I introduced The Peter Kiewit Institute (PKI) as one of the Nation's premier educational institutions. This edition presents several articles describing a few of the programs and opportunities available at PKI.*

And with that theme of education, we are pleased to present a number of other articles focused on information assurance (IA) and higher education including the DoD IA Scholarship Program (IASP), the Information Warfare (IW) training available through the Unites States Military Academy and the U.S. Navy's Naval Warfare Information Warfare Staff and Operations Course.

Products

I've often said in this IATAC Chat to visit our Web site. I thought it might be useful to highlight some of the resources available through our Web site—http://iac.dtic.mil/iatac.

This section provides a summary of all of our core products [e.g., Tools Reports, State of-the-Art Reports (SOARs), Critical Review and Technology Assessment Reports (CR/TAs)]. For those entering the site from a .mil or .gov domain, they may download PDFs of those reports. We also post the IO Calendar as well as the IA Digest. The IT Product Evaluations (restricted to .mil and .gov) contains abstracts of all assessments done within DoD that have been posted to IATAC as well as procedures for ordering full PDFs of those reports. This section has recently been updated to provide keyword searches.

Services

This section of the of the Web site presents the processes and procedures for ordering Technical Area Tasks (TATs) and Subscription Accounts as well as describing some of the other services available from IATAC (e.g., training courses and conference and meeting support). One unique element of this particular section are the abstracts of work completed under the TAT program. Users may wish to examine this section for relevant materials that may assist them in their missions. Requests for full documents must be forwarded to IATAC and secondary distribution instructions will apply and be strictly adhered to.

For those wishing to initiate an inquiry, simply point and "click here" and an E-mail will be generated to our core E-mail address (iatac@dtic.mil) and we will initiate research accordingly. Note that our basic inquiry service is limited to four hours of research. Extended, Search and Summary, and Review and Analysis services are on a cost recovery basis.

News and Events

In an effort to facilitate the ease of navigating through our Web site, we've also included both the IO Calendar and IA Digest on this sub-menu. The Success Stories are highlights of work done under the TAT program.

Resources

We've developed a growing list of important Web sites as a ready reference for jumping to additional resources. No doubt it is not all-inclusive, so if there are others, please drop us a note so we can post them.

Help Desk

This is an assortment of resources for initiating inquiries, a listing of other inquiries we've had in the past, which may assist you, as well as contact information for IATAC. Visit our site frequently as we are currently in the process of revamping it. In the upcoming month, viewers will be able to search by keyword through our products and the IT evaluation sections.

Finally, you can also access us via SIPRNET at https://iatac.dtic.smil.mil.

by John B. Callahan, Jr. and Steve Stock

Student oriented, industry driven, the Peter Kiewit Institute (PKI) merged students, faculty, business, and government to launch the international launch of the Lewis and Clark bicentennial database server and event welcome Web site. Together with the U.S. Army Corps of Engineers, the National Parks Department, area commerce, and other various local and Federal agencies, Kiewit students intertwined differing technologies, an assortment of users needs, and the burdens of a non-traditional college environment that meant relying on colleagues in various specialties, to produce a product flexible and reliable enough for scholarly research, but also aesthetically appealing and friendly for a more casual client, while delivering guaranteed availability to a site that has the potential for 100,000 hits per day.

Our vision was of a center of development for young minds that will truly lead the way for the technology of tomorrow…and with this Lewis and Clark project, it is yet another example of how education and industry working together can not only ride the next wave of ingenuity and invention, but create and mold the direction of technology.

Walter Scott, Jr.
Chair PKI Board of Policy Advisors
Chairman, Level (3)

Using as a basis the unique relationship the Institute has with multinational industry, as well as the working understanding that it shares with several branches of the Federal government, PKI was able to procure the assignment to design, administer, and develop the architecture of the Web site that has been the foundation of the overall celebration of exploration that the Nation has been undertaking since the beginning of the 21st Century. Its goal was to be a hub, where every type of neo-adventurer, from the Lewis and Clark enthusiasts who wanted to contribute a piece of memorabilia, to the descendant of a pioneer who might have an anecdote that has been passed through generations, to the family wanting to plan an educational summer excursion, would gather and submit data.

This site needed to be the epicenter of activity for the country to reference. We needed technology powerful enough to support researchers that would both query the site and tender their own contributions. We needed a site that would provide maps and agendas for local activities throughout the nation. We also needed a destination for elementary aged children, where they could learn and explore while having fun. PKI has delivered on all fronts.

Johnette Shockley
USACE Peter Kiewit Institute
Transfer Coordinator

The challenges for students working on this scale, facing real deadlines and deliverables while working with a technology that is developing, were obvious—but so were the rewards. The mission of the Kiewit Institute since its inception in 1997 has always been two-fold—

- To provide the Midwest with the information technology personnel it so desperately needs to support rapid economic growth in an information economy.
- To give students the opportunity to work in an environment where they were not bound by the restraints of theory and could apply their knowledge on actual business problems.

With the Lewis and Clark project, which, among its other endeavors, already has had a major motion picture produced in conjunction with the commemoration, PKI was given the chance to test this university-to-industry experiment on a grand scale.

The students were paired with faculty advisors and liaisons from industry and government. Working through new and innovative learning mediums, from traditional college classes to small groups which acted as a small business would, with budgets, client briefings, and results-based pay, gifted students were given the chance to program, main-

tain the system and consult subject matter experts on the design and architecture of the Web site. The Web outlay, the graphical user interface, the twelve terabyte database storage configuration, the networking configuration, the construction of the hardware, the analysis and design of the architecture, the security, the maintenance—were all done by students, each learning and working with different operating systems and software—each having to connect their unique piece to the whole in under one calendar semester.

The various clients an their need for different software solutions compounded the complexity involved with any education-based initiative, or government-based for that matter. Products from IBM, Microsoft, ARCIMS, Network Appliance, Red Hat, Dell, Cisco Systems, and Intel were all utilized in the construction of the site, sometimes by students with no previous experience with these technologies. Abstract ideas that few businesses have discovered to date were put into production, such as with the Linux Virtual Server (LVS). A highly configurable routing solution that provides the features of high availability and extremely flexible scalability at relatively no cost to the University. LVS is just one of the burgeoning technologies PKI students are integrating into pioneering businesses to inexpensively bridge the digital divide.

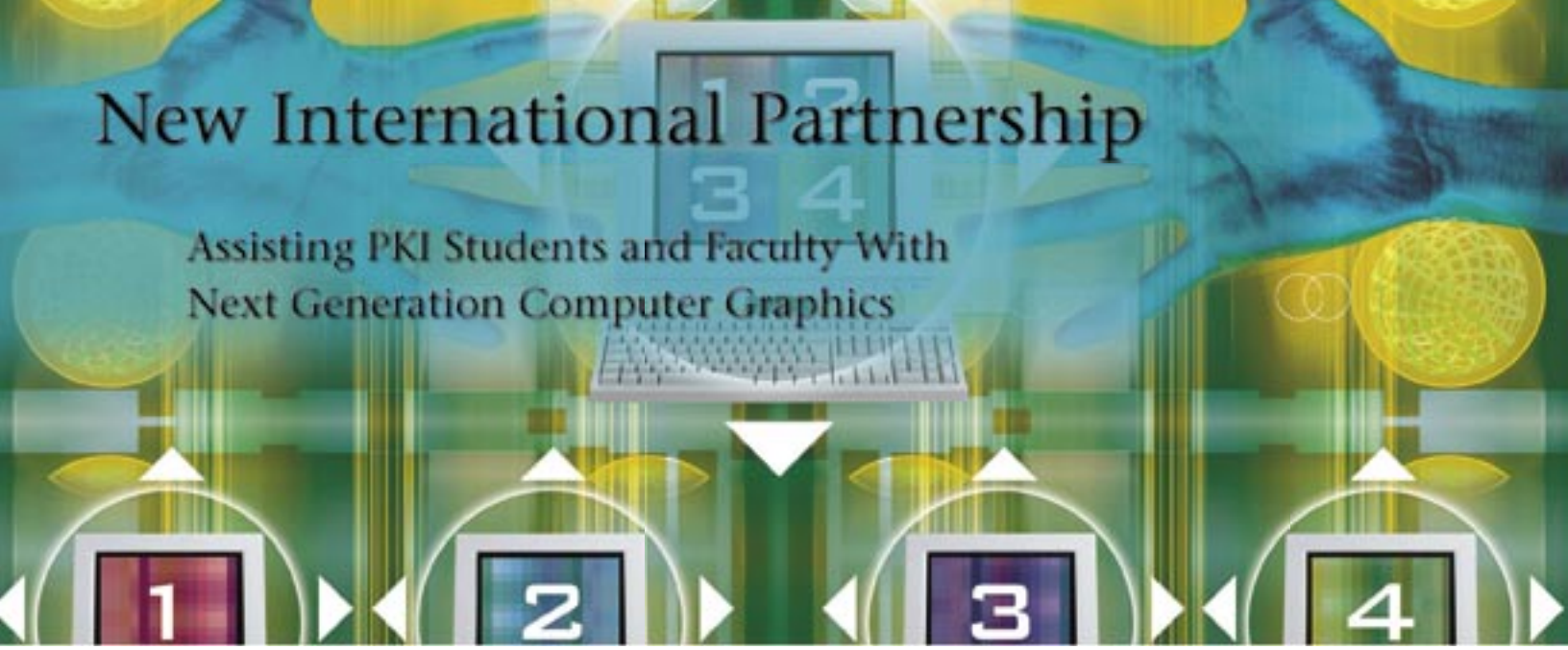
This high tech, cost effective solution creates an environment that exceeds all our original goals, and provided students with an opportunity to learn about routing and load balancing on high traffic Internet sites from the inside. The students learned through the experience of building and configuring the entire infrastructure and had fun doing it.

Steve Stock
Senior Technology Research Fellow and
Chief System Architect

This range of technical advancement was necessary to host the scope of what the student web designer had in store for the layout, which would incorporate every visual and audio means to take the user back to the days of the Louisiana Purchase. The key element of the page is the journal of the day, which will communicate the thoughts of the adventurers on the corresponding date two hundred years ago, with the explorers of today. Researchers can use the most comprehensive Lewis and Clark search engine in the world to further their studies, while collectors can use the same technology to donate their treasures to the project. Children can watch educational videos on the history of the trail, the explorers and the Native Americans who aided in the creation of our frontier. Families and historical groups can use the interactive geographical survey map feature provided by the ESRI Corporation to plan trips or simply view the topology that voyagers overcame in route from Missouri to the end of the Oregon Trail. The maps, provided by satellite images from the Corps of Engineers, pinpoint areas of interest along the way where the expedition trekked, and these graphical locals are linked with event pages and calendars corresponding to their placement both geographically and historically.

The backbone of the system is two-fold—with the storage needs handled by a twelve terabyte Network Appliance Network Attached Storage unit, which allows the Web servers to communicate with a massive DB2 database which houses all of the information mined out to the site. The second major component of the infrastructure is an IBM p–670 computer that acts as the actual database for the system, handling any queries, updates, or submissions from outside sources. The entire configuration valued at over $6 million was made possible entirely through grants and donations from visionary companies that are leaders in their industry and which have continuing partnerships and research commitments within PKI.

continued on page 13



by John B. Callahan, Jr.

In the spring of 2003, The Peter Kiewit Institute (PKI) became a charter member of the imedia International Certificate Program for New Media (ICPNM), which strives to bring fresh and innovative interactive media technologies to industry through a series of educational partnerships and accreditation seminars. PKI will work closely with the Fraunhofer Center for Computer Graphics, the Rhode Island School of Design, and the Technical University of Darmstadt (Germany) to not only bridge exciting new frontiers for students in Nebraska, but give the "best and brightest" of the Midwest a chance to give back to the world.

The goal of the program is two-fold—to provide instruction on truly cutting-edge graphical technology, but to also foster innovation, creativity, and the type of "outside the box" thinking that leads to great discovery. Experts from around the globe in visual design, graphical art, computer science, cultural science, and business have all been assembled in this program to give each participant the most holistic view possible, while in turn, providing them the opportunity to learn and grow with the program.

Under the agreement, PKI will send no less than two faculty members or students a year to the Academy, where they will go through a rigorous nine month program focusing on the aforementioned specializations under the direction of imedia's staff. Each member will have the chance to design their own particular curriculum, ranging from work with structured multimedia, live Web sites, 3-D worlds and virtual reality, including studies in animation, 3-D modeling, interface design, hypermedia, and a wide array of interactive digital media tools. The participants will undergo five months of classroom instruction and four months of practical internships, after which they will present a final project to a group of distinguished judges.

A further benefit from the memorandum of understanding is the placement of PKI faculty and Omaha area business leaders on the Board of Directors and the Steering and Accreditation committees for the program. Constructed in a similar fashion as the PKI Board of Policy Advisors, ICPNM's steering committee consists of half industry heads and half academia, while the accreditation members will be that of solely PKI faculty, allowing the University of Nebraska to become a center for interactive media excellence and training.

With this new relationship, The Peter Kiewit Institute has the ability to drive the direction of a vastly expanding medium while taking advantage of top-notch educational equipment, personnel, and facilities to benefit students. ■

About the Author

John B. Callahan, Jr.

Mr. John Callahan worked with systems architecture under the direction of Steve Stock during his senior year. His effort in this area was one of two independent studies he undertook in an effort to broaden his knowledge base and determine areas of interest for future study. As a part of the work he did during the internship, he helped configure the operational construct needed for the Lewis and Clark Web site. John graduated from the University last May with a major in Management Information Systems. He begins graduate study at the Institute this fall.

If Seeing is Believing

Success is Evident at PKI

by Winnie Callahan and Ken Moreano

How do you determine success when evaluating a higher education initiative? There are traditional ways such as growth in student enrollment, caliber of professors hired, number of publications, research grants awarded, endowments, etc. The University of Nebraska's Peter Kiewit Institute can certainly tout these traditional measures, but with a motto like "moving at the speed of business," there are also some not so common indicators that provide clear proof that super things are happening.

For the purpose of this article we will review the physical plants, associated with this whole endeavor. It's not so much the number of buildings on the South Campus of the University of Nebraska at Omaha, but rather the speed with which they have been added.

In September 1997, ground was broken on the first of the structures located here. The 192,000 square-foot classroom and lab facility boasts of an exposed infrastructure to include fiber connections, routers, switches, wiring closets, and firewalls. In fact, an article appearing in *The New York Times Circuits Section* in August 1999 pictured the wiring closets and talked about the unusual glimpse this gives students of computer science, information technology, or telecommunications. The *Times*' position was that the exposed infrastructure in this facility showed students how a building is built for the internet age.

From the groundbreaking on this first complex structure to its completion in August 1999, not two years had passed. Late October 1999, big machines once again moved dirt, this time an honors residence hall with 164 private bedrooms designed around 4-bedroom suites and a state-of-the-art conference center were moving from the drawing board to reality.

Students began occupying the second and third structures in mid-August of 2000. The residence hall has broad bandwidth capability and large lounges for group collegiality, while the conference center is completely built on raised flooring and has ceiling mounted projection equipment, smart board, a distance learning styled boardroom and provides tremendous flexibility with movable walls, different furniture types, food service division, and other wonderful appointments. The capacity of the conference center is roughly 600 but does vary based on furniture choice and room arrangement.

To support the growth of incubator start-up companies and to provide space for shared research projects with other institutions and/or business partners, a research-technology transfer facility was built beginning in October of 2000. With around 60,000 square-feet of lease-ready space, a rich mixture of companies from those just starting from a student project to corporate giants soon filled the first phase of what was designed to be a two-phased project. The first tenant moved in early December of 2001; the building is currently fully leased and/or occupied by partners deemed appropriate to the disciplines taught at the Institute. The "mixed-bag" approach has already begun to result in sharing and joint contracts between and among the roughly 23 tenants and the two Colleges in the Institute and/or the University of Nebraska's Medical Center as well.

With the broadband connectivity which will take the campus "on-net" with Level 3 and the two IBM super computers engaged to support a variety of projects (both Level 3 and IBM are partners with PKI) already identified, interest and momentum continues to grow.

Phase II is scheduled to get underway within the next 30 to 45 days with more than 50 percent of that facility already promised. A third and fourth structure are in the planning stages and groundbreakings are expected on both prior to winter this year.

As visitors come and partners sign-on, comments reflect surprise that The Peter Kiewit Institute, true to its name, is "moving at the speed of business." And if you don't believe it, come count the bricks! ■

continued on page 13

Building a Parallel Password Cracking Environment

A Case Study

by Jeff Lunglhofer

In the 1950s, the dawn of the true computer age, complex computer systems were physically huge, enormously expensive, and working with such a system required highly trained operators, scientists, and small armies of computer programmers.

As the technology progressed, faster computer systems were packed into smaller and smaller packages, and made more affordable. That trend, which continues today, led to the introduction of widely available and affordable personal computers (PCs) in the early 1980s. Most PC users do not require massive amounts of processing power to fulfill their day-to-day computing needs. While everyone yearns for the "fastest" computer available, the fact is that the central processing units (CPUs) of most PCs are idle the majority of the time.

In addition to the average PC user, there is also a smaller group of computer users that perform incredibly challenging computational tasks. These users are primarily found in scientific communities, and the tasks performed range from nuclear weapon simulations to weather prediction and modeling. These users require the highest possible performance to get the maximum benefit from computers.

Enter supercomputers

The power-hungry user community currently has a variety of options to choose from in fulfilling their computational needs. Several vendors offer very high-end computing platforms that contain multiple CPUs, shared system memory (in some cases), multiple data buses, and many other innovative means to accelerate performance. Even today, these types of systems are typically proprietary in nature, need specially coded software, and often require that software be compiled with special software compilers. While this may seem daunting, the performance yields from these systems can be phenomenal. For organizations that can afford the staggering expense of purchasing these kinds of supercomputers, maintaining the expertise to develop applications is not an issue. But these kinds of well-funded organizations are not the only ones with the need for extreme processing power!

Enter cluster computing

Cluster computing is the process of taking multiple stand-alone computer systems and chaining them together in such a way that they are able to take advantage of their aggregate processing power. The technology used to develop computer clusters is not new and borrows heavily from the realm of true supercomputers. In fact, many supercomputers operate in a fashion that is strikingly similar to a cluster-based environment, which significantly blurs the lines between supercomputing and cluster-based computing. Since many clusters are constructed with commercial off-the-shelf (COTS) products such as simple rack mount or desktop PCs, they are typically not reliant upon proprietary hardware/software solutions. Of course, abandoning specially designed hardware/software can also have a significant negative impact on performance. For many applications, however, this drawback is more than made up for with the high performance verses cost ratio that can be achieved with a relatively simple cluster design.

Problem—Password cracking

Often, during the execution of a security assessment (particularly penetration testing), it is desirable to rapidly crack password hashes that have been harvested from a compromised system. Password cracking is an enormously CPU-intensive activity, since trillions (or more) of keys must be processed in order to perform a complete brute force attack (checking all possible passwords). Clearly, this problem is an excellent candidate for some form of super-

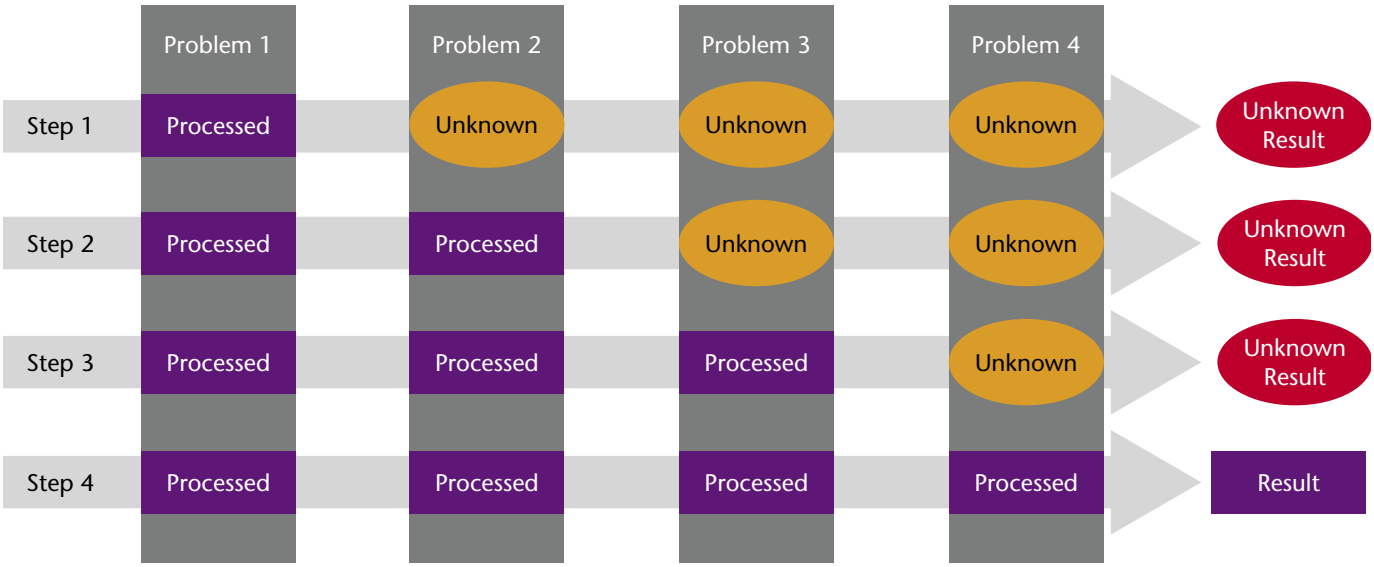


Figure 1. Serial processing

computing. Given the surplus of older desktop computer systems, the low cost of deployment, and the desire for the exercise to be a learning experience, a cluster-based system was chosen as the platform on which to support a parallel password cracking application.

Building a clustered environment

A standard, stable, and scalable cluster environment was chosen to address the password cracking issue. Standardization was highly desirable, so that it is possible for the cluster to be used for additional applications and projects at some point in the future. Linux was selected as the base operating system. Linux is ideal for building a High Performance Computing (HPC) environment since system developers have full access to the Operating System (OS) source code. Modifications to the OS are often the only means by which many key features can be enabled.

Two "supercomputing" style features are offered, as the cluster is currently deployed, from which applications can benefit: massively parallel processing (MPP) and single system image (SSI). Both offer a different model by which an application may take advantage of the aggregate processing power of the cluster. Only SSI will be addressed here, as this was the mechanism selected to facilitate parallel password cracking.

Single system image (SSI)

In simple terms, SSI allows all the individual computer systems that make up a cluster to share process space. This means that almost any program running on a particular node can "migrate" to a faster, or less loaded node to improve that application's performance. There are several SSI packages available, but an open source version of multicomputer operating system for Unix (openMosix) was selected due to the intense on-going development efforts, strong user community, and the open source licensing of the software. OpenMosix enables SSI by patching the Linux kernel. At the time of this writing, the most current release

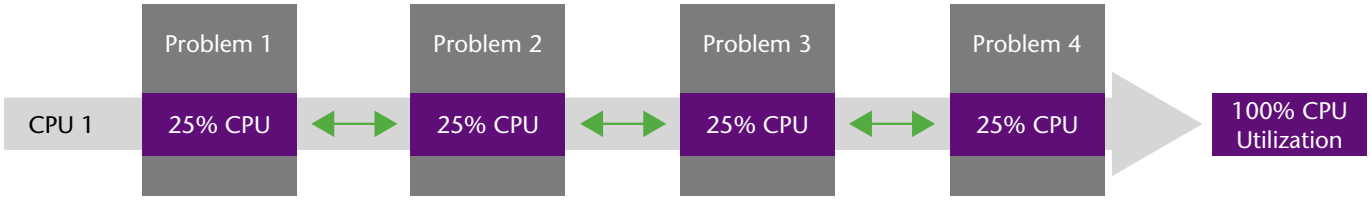


Figure 2. Four serial programs on a single CPU.

of openMosix is 2.4.20–3, and includes patches for the current stable 2.4.20 Linux kernel. While SSI is a powerful tool, it is important to recognize the limitations of this technology. The vast majority of software that is currently available is written to process serially, that is to sequentially solve problems. Figure 1 (see page 9) illustrates serial processing.

Note that each problem must be solved prior to beginning work on the second problem. An individual program that solves problems in this way will not benefit significantly from having access to multiple processors. The strength of SSI becomes evident once it is necessary to run multiple CPU-intensive processes such as the one illustrated above. Individually, they cannot benefit from multiple CPUs, however, each process can easily be migrated out to an available processor to realize a significant performance gain. Figure 2 represents several serial programs being run on a single CPU. Figure 3 illustrates those same programs being load-balanced across a cluster via process migration.

Note: The vast majority of programs written for PCs are unable to take advantage of multiple processors. That's right, buying a Symmetrical Multi Processor (SMP) motherboard will not make (most) games perform significantly better!

As this diagram demonstrates, using an SSI cluster yields a significant performance boost by balancing the processing load across all cluster nodes. Note, however, that a single program will run at the same speed on this cluster as on an unburdened stand-alone computer system (assuming similar CPU speeds, etc.). A program must be specifically written to be able to take advantage of all available CPUs. Typically, this is accomplished by creating multi-threaded applications.

What is this "thread"?

In simple terms, a thread is merely a piece of a program that is instructed to "break away" from a main program to perform some work as a separate, but connected entity (or thread) of the main program. Threads are often instructed to solve a particular piece of a problem, and then report back to the master process with the results. On systems where multiple CPUs are available (such as on an SSI cluster), this is an excellent way to take advantage of multiple CPUs to more quickly solve complex problems. Individual threads can simultaneously solve problems leveraging different available processors. Figure 4 (see page 14) demonstrates the concept of splitting out workload between threads.

Selecting a password cracking program

With the openMosix SSI cluster built, the next step was to select a cracking program to use as a basis for development. Several password crackers were identified that are intended for cluster environments, or a distributed network environment. Several were evaluated, but they suffered from poor performance and a lack of features. John the Ripper, a password cracker, was selected for its flexibility, high-speed capability, and because it does not have an efficiently implemented parallel password cracking mechanism built in. This made John the Ripper ideal for the project. Before beginning the process of multi-threading the application, it was necessary to first identify a methodology for password cracking.

Parallel password cracking—A methodology

Most modern password systems utilize cryptographically strong algorithms that resist attempts to determine the encrypted data without first guessing the "key" (e.g., password). Thus password crackers usually perform several types of password checks in an effort to identify the valid key, and thus crack the password. The first is to check a password hash against a set of pre-determined guesses. This is known as a dictionary attack, and can usually be performed quickly. Hybrid attacks work by making preconfigured modifications to dictionary words to generate password guesses. For example, the dictionary word "password" might be modified to "password1." People commonly make minor modifications to common words to formulate their passwords, and thus, this is a highly effective way to guess passwords. The last, and by far the most computationally challenging password cracking method is known as brute force cracking. Using the brute force method, every possible password guess is generated, run through the appropriate algorithm, and verified against the known password hash. For some hashing algorithms, this possible number of guesses is staggeringly high, and even with all the computers on earth, it should be computationally inconceivable to crack. For others, some of which are commonly deployed password mechanisms, given enough processing power, a thorough brute force attack is possible to accomplish in a fairly short time.

In the description of password cracking mechanisms above, we note that by using some algorithms it should be impossible to crack a password. That makes the assumption that humans select truly random passwords, which is a big assumption! Humans, in fact, rarely select truly random passwords. A study of over 7,000 passwords by a security assessment team revealed some startling information.

Humans and their passwords

It is a fairly common belief that most people have difficulty remembering sequences of numbers that extend beyond seven in length. It has been suggested that this may be one of the reasons that telephone numbers in the United States were originally seven digits in length. Passwords that appear to be truly "random" rarely exceed eight characters in length. Passwords longer than 8 characters are almost always a derivation of a known dictionary

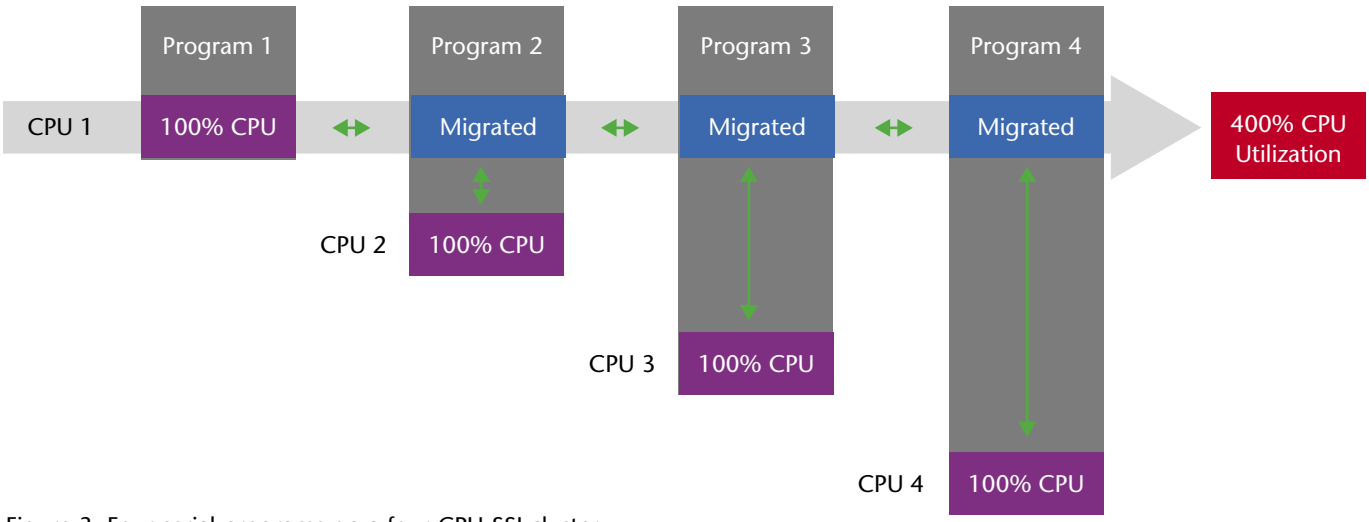


Figure 3. Four serial programs on a four CPU SSI cluster.

word, or of a word/acronym associated with the individual or the individual's employer. Dictionary and hybrid attacks are very effective at cracking those passwords. Often the more difficult passwords to crack are the "random" seven or eight character passwords.

However, the weak cryptographic system employed by many systems to "protect" user passwords have some significant flaws (sometimes called "features") that allow for the current cluster to perform an almost comprehensive brute force attack in a matter of days on passwords ranging from zero to 14 characters. Many users create weak passwords and reuse them on multiple information systems—this compounds the problem by providing attackers with access to many systems after cracking a single password.

When random isn't really random—Password profiling

A cursory analysis of user passwords reveals that the vast majority of passwords are still based upon dictionary words, and thus are likely to be cracked by a dictionary and/or hybrid password cracker. The remaining "random" passwords share some common traits. For example, in some user communities, checking passwords that follow some basic rules can net close to 90 percent of "random" passwords. One possible rule-set might be—

- Total password length is 8 characters
- Contains no less than 1 digit and no more than 4 digits
- Contains no less than 1 capital letter and no more than 2 capital letters
- Contains no less than 1 vowel and no more than 4 vowels
- Contains no less than 1 consonant and no more than 4 consonants
- Contains no less than 1 special character and no more than 3 special characters (e.g., !, #, etc.)

While this is not a particularly granular example of password profiling, it is possible to crack passwords matching more specific guidelines. This method is particularly useful when it is possible to obtain the password policies of the organization associated with the password hashes we are trying to crack. Often these guidelines are publicly available as part of an organization's security policy, and are certainly available to an insider.

Even with the use of password profiling there are still a large sum of password guesses to be attempted, which means that the more processing power available, the better. This brings us back to the cluster!

Teaching the "brute" in brute force

Cracking passwords that comply with rules is relatively trivial, and many password crackers already have methods built in to accomplish this task. These implementations, however, vary significantly in quality and efficiency. Because of the learning objectives of this exercise, simple password generation routines for a semi-intelligent brute force password generator was developed to feed the results into the John the Ripper password cracking engine for processing. The resulting code is simple, and operates in the following manner—

- Create arrays, one for each character set that correlates with a rule
  - Example:
    lowalpha[26] = "a","b","c","d","e","f","g"…
- Determine the total possible unique arrangements of these arrays to satisfy the rule requirements
  - Example:
    position1 = lowalpha, position2 = digit.…
- Begin with the first arrangement, and check value[0] in each array as the starting password to check
- Increment the first position's value, generating the 2nd password to check
- Continue until the array in the first position overflows
  - Increment the second position array
  - Reset position 1 to value[0]
- Start over until all positions have been exhausted, then begin again with a new arrangement.

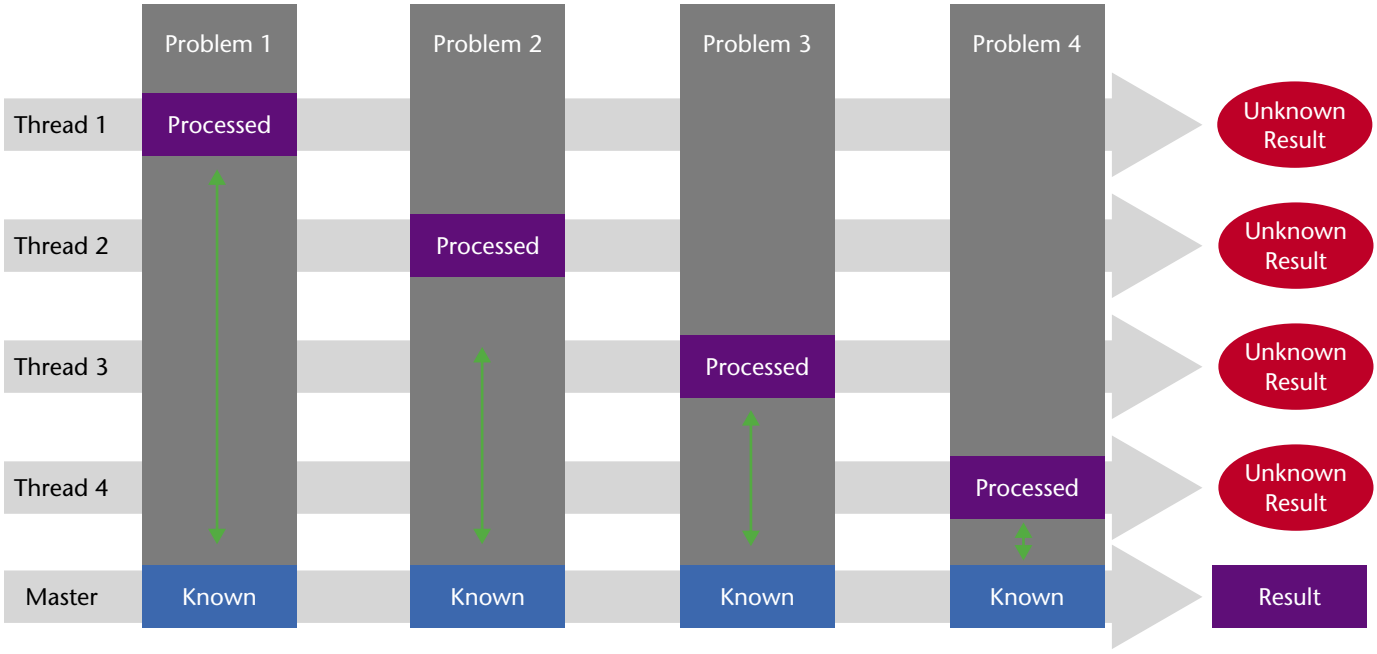


Figure 4. Multi-threaded application.

While this method is fairly good at performing an intelligent brute force attack, it does not lend itself well to operation in a parallel processing environment due to the sequential method used to generate password guesses. What is missing, at this point, is a method to easily identify blocks of passwords for assignment to individual program instances, or threads.

A simple methodology for parallel brute force password cracking

To perform cracking in parallel, it is critical that each program thread never duplicate the effort of another thread. Each thread should compliment the others, with one thread picking up where another will leave off as the overall cracking effort progresses through the entire key space. One solution to this problem is to have a simple method for each program thread to quickly identify where the last thread to request a key block will stop cracking, begin cracking from that point, and crack a configurable number of password guesses. Thus the total passwords processed by a single thread are known as that thread's key block size.

This technique is fairly simple and seemed easy to implement, and was thus selected as the method for "refereeing" key blocks assigned to a configurable number of John the Ripper password cracking threads.

Putting it all together— Threading John the Ripper across the cluster

Implementing the method for parallel cracking outlined above required some relatively minor modifications to the source code of John the Ripper. Once completed, John the Ripper was configured to crack passwords in parallel by creating multiple threads, each one of which was assigned unique key blocks. Once a thread completes its assigned workspace, it simply obtains its next block assignment from the master process and continues on. On the SSI cluster described above, 32 threads are created and automatically load-balanced across the cluster. Given the relative lack of bottlenecks with this implementation, the performance of this multi-threaded implementation of John the Ripper almost precisely equals the speed of multiple independent instances of John the Ripper running on isolated systems. For example, the cluster performance against unsalted hash types (such as those commonly used to store passwords on Windows platforms) peaks around 82,000,000 guesses per second. Against a more challenging hashing method, such as salted Data Encryption Standard (DES) (commonly used by many Unix flavors) performance against a single hash peaks around 15,700,000 guesses per second. While those numbers may not be terribly impressive in and of themselves, consider first that many of the cluster nodes on the cluster are older Pentium II and slow Pentium III computers. While the cluster currently boasts a modest 32 processors, the maximum number of processors and nodes is theoretically in the thousands. Password hashes beware.

Conclusions

In the last decade, cluster computing has not only become a viable option for creating a supercomputing environment, it has also become a far more affordable and obtainable technology. Fairly impressive arrays of CPUs can be developed with underutilized "retired" PCs in many cases, and just imagine the performance possible with a modest investment in a large number of modern computer systems. This case study reveals that achieving high performance in a budget-conscious environment is very possible, and that the possible applications for this technology are virtually limitless.

The lessons learned from an Information Assurance (IA) perspective are chilling. As IA professionals, we need to more widely recognize the severe limitations of the username/password model. Newer and better technologies exist for performing user authentication, such as biometrics and Public Key Infrastructure (PKI). We should collectively explore the use of these new technologies to assure that we

continued on page 17

…continued from page 5

"The Peter Kiewit Institute (PKI)

From the conception of the Institute, the business community, both locally and throughout the world, have stepped up and made these students ideas a reality through their generosity. From IBM and Network Appliance, to here in Omaha with First National Technologies, companies have made major contributions to the success of this project, our students and to improving the quality of education as a whole. I think this project really emphasizes the objective of this program we have at PKI—bringing together people from diverse backgrounds, with diverse skill sets and putting them to work on one common goal. That's how the business world works and that is the environment we strive to create here for students.

Winnie Callahan
Executive Director of the Peter Kiewit Institute

With over 100 students, from over a dozen countries, working with nearly fifty government agencies and businesses, putting in extensive time to meet the bicentennial kick-off, there is no doubt that this was not simply another university academic exercise, but rather an opportunity for students to network, learn and create with influential members of industry and world-class faculty, and to continue to lead the voyage of discovery into the next two hundred years.

"The same spirit that drove our nation and its explorers over two centuries past, I want to instill in our young people today," Scott said. "Not only to learn but to take that knowledge into bold new frontiers in order to help their fellow man." ■

About the Authors

John B. Callahan, Jr.

Mr. John Callahan worked with systems architecture under the direction of Steve Stock during his senior year. His effort in this area was one of two independent studies he undertook in an effort to broaden his knowledge base and determine areas of interest for future study. As a part of the work he did during the internship, he helped configure the operational construct needed for the Lewis and Clark Web site. John graduated from the University last May with a major in Management Information Systems. He begins graduate study at the Institute this fall.

Steve Stock

Mr. Steve Stock is the Senior Technology Research Fellow and Chief System Architect for the College of Information Science and Technology, one of the two colleges under the Institute umbrella. Steve came to the University of Nebraska at Omaha from Physicians Mutual Insurance where he served as Vice President and Chief Information Officer.

…continued from page 7

"If Seeing Is Believing…"

About the Authors

Winnie Callahan

Ms. Winnie Callahan is in her sixth year as Executive Director of The Peter Kiewit Institute and as Assistant Vice President of the University of Nebraska Foundation. She serves as a liaison between the business community, local leaders, the Deans of the two colleges in the Institute, and works with both UNL and UNO to enhance opportunities for collaboration and cooperation. She has taught both graduate and undergraduate courses and has recently received her doctorate degree in Educational Administration.

Previously, Ms. Callahan was with the Omaha Public Schools as a teacher, a building principal, and then in the Superintendent's office as Director of Public Information Services.

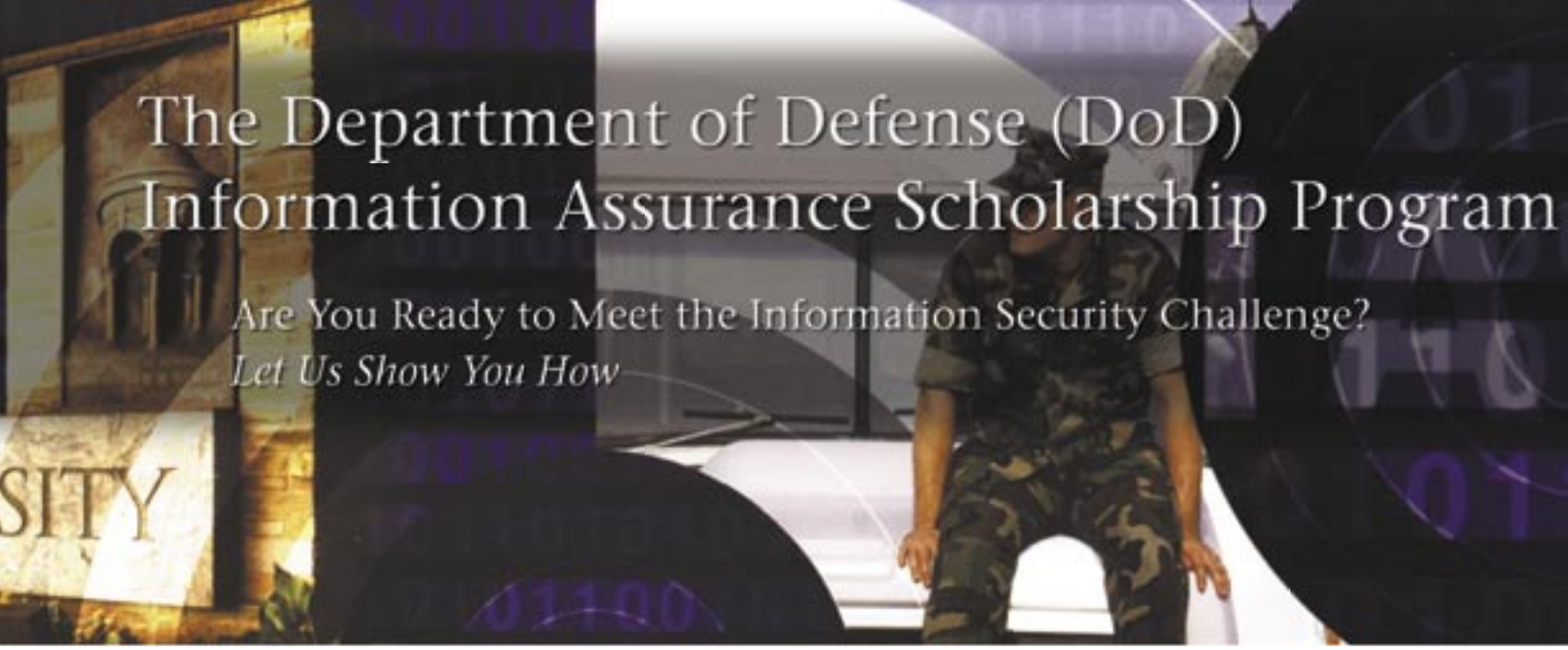
Ms. Callahan serves on a wide array of community boards having been elected president of several. She has received numerous recognitions to include the Nebraska Literacy Award and the YWCA's Outstanding Woman of Distinction Award. In addition, she has been a frequent speaker locally as well as nationally on a variety of topics. She may be reached at wcallahan@foundation.nebraska.edu.

Ken Moreano

Mr. Ken Moreano has been Director of the Scott Technology Transfer and Incubator Center for just over one year. As Director, Ken works under the guidance of the Suzanne and Walter Scott Foundation and with both the Incubator and Technology Transfer corporations. Ken works in partnership with The Peter Kiewit Institute and local leaders to promote economic development and entrepreneurship.

Ken also serves as a business development resource as well as a conduit for The Peter Kiewit Institute, The University of Nebraska system, and the Greater Omaha Chamber of Commerce in a variety of opportunities for collaboration and cooperation.

Prior to Ken's involvement with the Scott Technology Center, Ken was the founder of an early stage technology company, established in Austin, Texas (1998). Ken served as the founder and primary fundraiser while also directing business development/strategy. Ken can be reached at kmoreano@scott-technology.com.



by George Bieber

We're meeting the information security challenge

Given our increasing reliance on information technology (IT), the growing threats to information, and information systems and infrastructures, it is critical that the Department of Defense (DoD) protect itself. To do so, DoD must be staffed with technically savvy personnel. The Information Assurance Scholarship Program (IASP) was established to help achieve this objective.

The Office of the Assistant Secretary of Defense Networks and Information Integration (ASD/NII) sponsors the DoD IASP with support from the National Security Agency (NSA) as the Executive Agent. Piloted in academic year 2001–2002, the objectives of the program are to promote higher education in all disciplines of information assurance (IA), to enhance the Department's ability to recruit and retain IA and IT specialists, to increase the number of military and civilian personnel in DoD with this expertise, and ultimately, to enhance the Nation's IA posture.

What is IASP?

The IASP is both a scholarship program for DoD, and a capacity building tool for the nation. The program is a result of commitment from DoD and Congress to support higher education as a means to prepare the DoD workforce to deal with threats against the Department's critical information systems and networks.

Recruitment scholarships (Non-DoD employees)

As a recruitment tool, the IASP sponsors students who currently are not DoD or government employees and who are enrolled in or applying to universities designated by NSA as Centers of Academic Excellence (CAEs) in IA (see Table 1). Scholarships for recruitment students are provided for Bachelors (Junior and Senior year only), Master's, and Doctoral degrees in an IA-related discipline.

Following graduation, students are eligible for full-time employment with various components and agencies across DoD. Students are required to work for DoD a minimum of one year for each year of scholarship support they receive.

Retention scholarships (DoD employees, civilian, and military)

The IASP supports DoD civilians, military officers, and enlisted personnel who pursue Master's and Doctoral degrees in IA-related fields of study. Typically, these retention students attend a DoD School designated as a CAE and, depending on the program, may finish their graduate degrees at a partnering university. For DoD civilian and military personnel, the service commitment following graduation is determined by their sponsoring component organization.

Retention program requirements and eligibility

Retention students have four types of opportunities for scholarship support—

- Information Resources Management College (IRMC) Chief Information Officer (CIO) Certificate Program and IA Certificate Program with follow-on scholarships—
  - **Program**—CIO Certificate Program and IA Certificate Program with scholarship support at an IRMC partnering university for Master's or Doctoral degrees
  - **Requirements**—Civilian GS–13 and above; Military 0–5 and above (may waiver one grade)

- Scholarships for IRMC CIO Certificate and IA Certificate Program Graduates—
  - **Program**—Scholarship support to attend a CAE for Master's or Doctoral degrees
  - **Requirements**—Completion of the CIO Certificate Program and/or IA Certification Program in FY01 or later and (Civilian GS–13 and above; Military 0–5 and above)

- Naval Postgraduate (NPS) School
  - **Program**—Master's and Doctoral degrees offered entirely through NPS
  - **Requirements**—Civilian GS 9–13 or higher; Military 01–06 (Most Services select 03 level officers)

- Air Force Institute of Technology (AFIT)
  - **Program**—Master's and Doctoral degrees offered entirely through AFIT
  - **Requirements**—Master's/Doctoral (civilian and military applicants, any grade); Doctoral (Master's in Computer Science/Engineering or closely related field)

Scholarship and capacity building grants

Three types of awards may be offered to participating CAE universities. A Basic Award covers scholarships and school program administration costs. Capacity Building grants, awarded in tandem with Basic Scholarship Awards, strengthen a school's faculty, curriculum, facility, and research development efforts. Lastly, grants to universities partnering with the National Defense University's (NDU) IRMC enable DoD civilians and military members to receive graduate IA education (via a scholarship) at a partnering school after completing IRMC's curriculum.

Academic Disciplines

IASP scholars may choose from an array of IA disciplines, including—

- Biometrics
- Computer Systems Analysis
- Information Security (Assurance)
- Computer Engineering
- Database Administration
- Mathematics
- Computer Science
- Electronic Engineering
- Software Engineering and more…

***A Center of Academic Excellence**—Information assurance education plays a critical role in producing the national information infrastructure. The Centers [CAEs] are key to having security solutions keep pace with evolving technology now and into the future…*

Dr. Lawrence Pettit
President, Indiana University of Pennsylvania

What are the benefits of the IASP?

- An opportunity for DoD Services and agencies to attract and retain top IA/IT talent
- Full scholarships for B.S., M.S., and Ph.D. degrees to individuals in IA fields of study
- Enhanced training and growth opportunities for current DoD civilian and military personnel
- Strengthened IA programs in academe through capacity building grants

What schools participate in the IASP?

The IASP is offered to qualified students at some of the nation's leading institutions of higher learning designated by NSA as CAEs in IA education.

The CAEs in IA Education Program is an outreach program designed and operated by NSA. The program goal

is to reduce vulnerability in our National Information Infrastructure by promoting higher education in IA and by producing an increased number of professionals with IA expertise in various disciplines.

There are a total of 50 DoD institutions and public/private universities recognized by NSA as CAEs in IA. The list below identifies the current DoD schools recognized by NSA—

- Air Force Institute of Technology
- Information Resources Management College (IRMC), National Defense University
- Naval Postgraduate School
- United States Military Academy, West Point

Public and private non DoD institutions are listed in Table 1.

The Information Resources Management College (IRMC), National Defense University (NDU)

IRMC, one of four DoD CAEs, boasts several certificate programs and academic partnerships with other CAEs. Through these alliances, retention students are able to enroll in one of IRMC's certificate programs and upon completion transfer up to 15 credit hours towards their degree requirements at a partnering institution.

Program offerings that link to the IASP include the Chief Information Officer (CIO) Certificate and the IA Certificate. For more information on IRMC and the National Defense University's Programs, please visit http://www.ndu.edu.

The following Web page provides additional information about the CAE program http://www.nsa.gov/isso/programs/coeiae/index.htm.

How many scholarships have been awarded to date?

Since its inception, the program has tripled in size, with more than 70 CAE students having received scholarship support during the first three years. DoD estimates awarding 30–50 new scholarships, and providing a follow-on year of support to approximately 20 current scholars during the academic year 2003–2004 competition.

How do DoD civilian employees or military members apply for the scholarship?

DoD components will nominate qualified civilian employees and military personnel for IA scholarship opportunities. Civilian employees are to contact their component training offices regarding procedures to apply for this educational opportunity. Military members interested in the program should contact their Service's point of contact for officer professional development and must have their community manager's permission to participate in the program. Enlisted participation requires appropriate endorsement from cognizant enlisted personnel managers.

How can DoD components participate?

For the recruitment program, component billets (full time equivalents) are critical to the success of this program! Each year, components have the opportunity to identify billets to sponsor recruitment students for internship and full-time employment positions following graduation. Organizations may do so by responding to the Annual Call for Billets Memo issued by ASD/NII.

For the retention program, DoD components may nominate qualified civilian employees and military personnel for scholarship opportunities by responding to the Long Term Training Memo issued by ASD/NII.

If your agency is interested in participating in the program, please contact the IASP Program Manager, Christine Nickell, at 410/854-6206 or c.nicke2@radium.ncsc.mil for more information on how you can leverage this program.

Table 1. Public and private non-DoD institutions

Public and Private Non-DoD Institutions		
Auburn University	New Mexico Tech	University of California at Davis
Capitol College	North Carolina State University	University of Idaho
Carnegie Mellon University	Northeastern University	University of Illinois at Urbana
Drexel University	Norwich University	University of Maryland, Baltimore County *
East Stroudsburg University	Pennsylvania State University	University of Maryland, University College *
Florida State University	Polytechnic University, New York	University of Massachusetts at Amherst
George Mason University *	Portland State University	University of Nebraska, Omaha
George Washington University	Purdue University	University of North Carolina at Charlotte *
Georgia Institute of Technology	Stanford University	University of Pennsylvania
Idaho State University	State University of New York, Buffalo	University of Texas, San Antonio
Indiana University of Pennsylvania	State University of New York, Stony Brook	University of Tulsa *
Iowa State University	Stevens Institute of Technology	University of Virginia
James Madison University *	Syracuse University *	Walsh College
Johns Hopkins University	Texas A&M University	West Virginia University
Mississippi State University *	Towson University	
New Jersey Institute of Technology	University of Dallas	

* Denotes partnering universities with Information Resources Management College National Defense University (IRMC/NDU)

IASP Student Satisfaction Ratings

- *When asked to rate their overall satisfaction with IASP, 82 percent of students report that they are very satisfied with the program.*
- *All students who completed an internship gave favorable responses when asked to rate their overall impression of DoD as a place to work.*

How can I find out more?

The IASP is evolving to include distance learning opportunities, part-time programs, and increased DoD civilian participation. For a full listing of participating schools, eligibility requirements, and more information on the IA Scholarship Program, please visit the IASP Web site at http://www.defenselink.mil/nii/iasp/. ■

About the Author

George Bieber

Mr. George Bieber is Deputy, IA Human Resources and Training, for the Defense-wide Information Assurance Program (DIAP). In this capacity he has oversight responsibility for all aspects of the Department's IA education, training, and awareness activities, including the DoD IASP, as well as IA manpower and personnel issues.

Previously, he served as Chief, IA Education, Training, Awareness (ETA) and Products Branch, Defense Information Systems Agency (DISA). He managed the development, production and dissemination of DoD IA training and awareness materials.

Mr. Bieber has been actively involved in a wide range of Federal organizations, committees and working groups addressing IA training and professionalization issues. He has served on the Federal Information System Security Educators Association (FISSEA) Executive Board, and was the FISSEA 2000 Educator of the Year.

…continued from page 12

"Building a Parallel Password Cracking Environment"

are able to meet our mission assurance requirements well into the future. ■

About the Author

Jeff Lunglhofer

Mr. Jeff Lunglhofer currently leads a team of penetration testers who proactively assess and report on the security posture of client networks. Since 1997, Jeff has had the pleasure of working with many organizations, ranging from the United States Navy and the National Aeronautics and Space Administration (NASA), to commercial entities. Jeff can be reached at iatac@dtic.mil.

References and Resources

Beowulf Underground http://www.beowulf-underground.org/
Parallel Virtual Machine (PVM)
http://www.csm.ornl.gov/pvm/pvm_home.html
Message Passing Interface (MPI)
http://www-unix.mcs.anl.gov/mpi/mpich/
openMosix http://openmosix.sourceforge.net/
Cray, Inc. http://www.cray.com/
OpenWall (John the Ripper) http://www.openwall.com/

State-of-the-Art Information Warfare (IW) Training

by MAJ Ronald C. Dodge, LTC Daniel J. Ragsdale, and COL Donald J. Welch

Author's Note: The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense or U.S. Government.

With the increased potential of a bona fide cyber terrorist attack and the possibility of a future "war in the wires," we must continue to improve the education, training, and resourcing of individuals responsible for defending our national borders—whether those borders are physical or electronic. The Information Warfare Analysis and Research (IWAR) laboratory at the United States Military Academy (USMA) has proven to be an exceptional resource for such an education for our students and faculty studying information warfare (IW) and information assurance (IA).

Critical infrastructure has been defined as those—

> *Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. [1]*

These industries could be significantly affected by a cyber-attack targeting industrial control systems such as distributed control systems and supervisory control and data acquisition (SCADA) systems. Examples of industry sectors that rely heavily on control systems are—

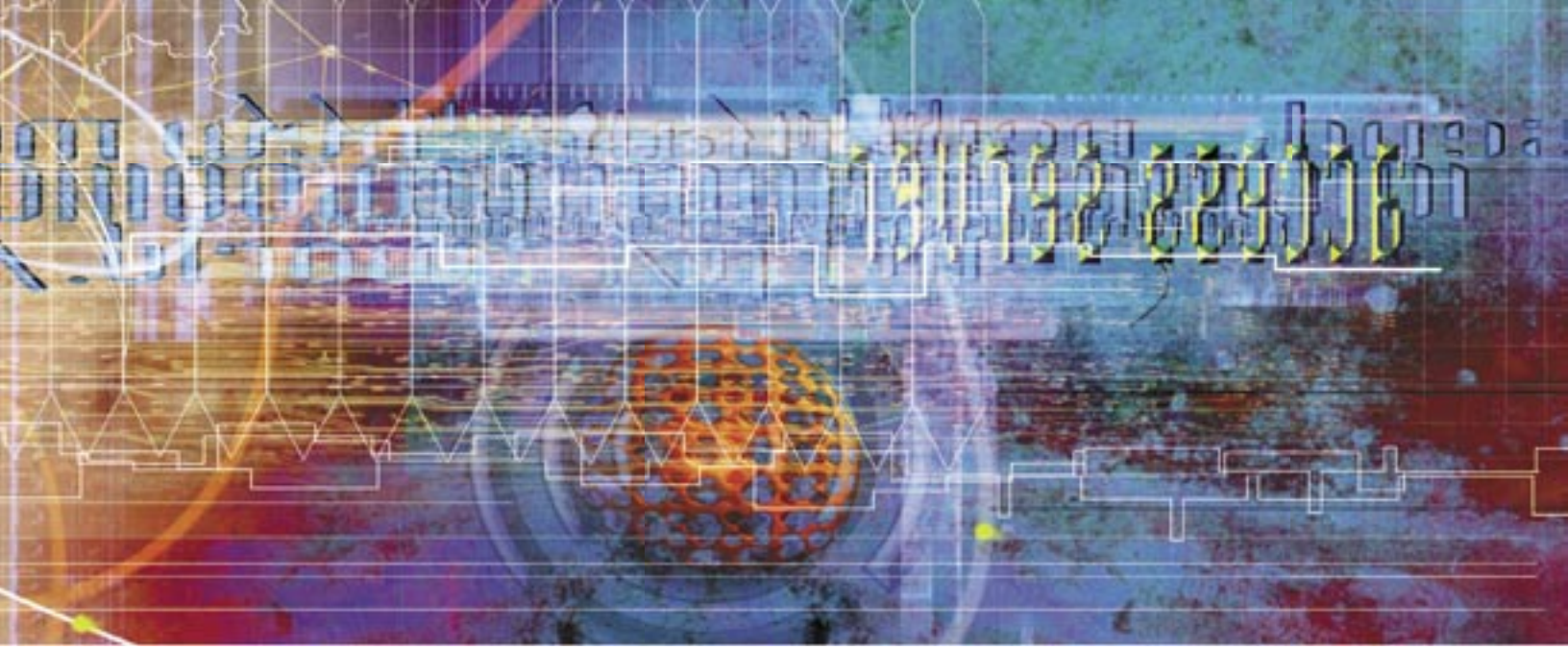
- Agriculture
- Food
- Water
- Public health
- Emergency services
- Power management systems
- Government
- Defense industrial base
- Information and telecommunications
- Transportation
- Banking and finance
- Chemicals and hazardous materials
- Postal and shipping [2]

National critical infrastructure and economic structure are becoming increasingly reliant on information systems and the Internet that provides connectivity between such systems. Cyberspace is the nervous system of these infrastructures—the control system for them.

While the silver bullet of network security doesn't exist, security can be significantly improved by uniformly applying current security methods. With the increased potential of a bona fide cyber terrorist attack and the possibility of a future "war in the wires," we must continue to improve the education and training of individuals responsible for defending physical and electronic systems.

Addressing these issues requires training in IA that does not merely theorize and describe such concepts, but provides students and users with a hands-on education. Much research and experimentation has been conducted in learning models with some of the most highly regarded models following a "hear—see—do" paradigm. It is estimated that in technical fields, people will retain only 26 percent of what they hear, 50 percent of what they hear and see, and 90 percent of what they hear, see and do. [3] A hands-on, active learning experience requires that we provide an environment where students, employees, and anyone managing or administering information systems can apply concepts in an isolated environment. Such an environment allows the unleashing of viruses, worms, and Trojan horses, but does not have an effect on a production network or the Internet. Kaucher and Saunders found that even for management-oriented graduate courses in IA, a hands-on, lab experience enhances the students understanding of theoretical concepts. [4]

USMA has, starting in 1999, built an IA lab that provides a robust suite of machines and services capable of supporting IA education and student/faculty research. The IWAR laboratory is comprised of several networks and subnets designed to provide a robust set of machines and networks to train on IA topics. [5] The lab configuration (see



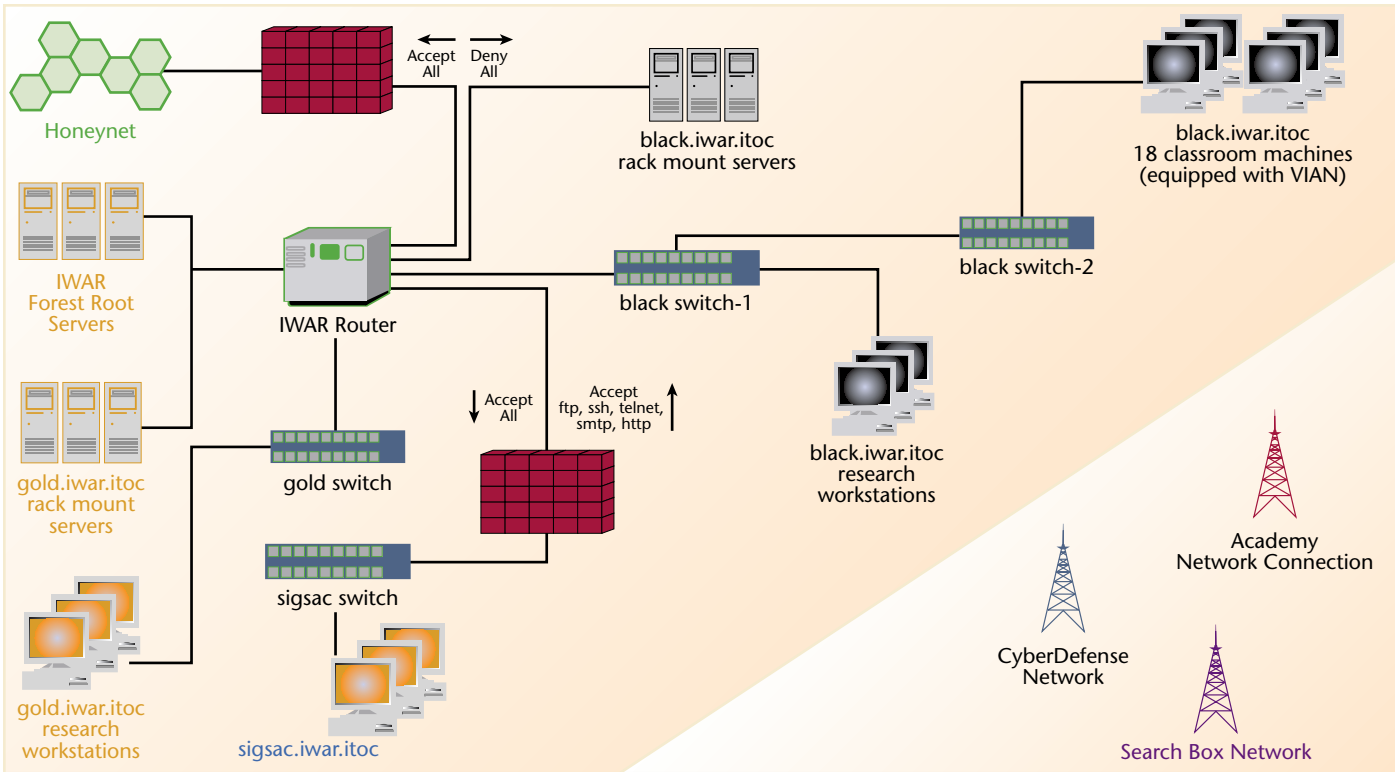


Figure 1. IW analysis and research laboratory

Figure 1) has evolved to combine a back end of stand-alone machines and servers with a series of student workstations.

The current network, representing approximately 200 nodes, primarily consists of two LAN segments based on the USMA school colors (gold and black) and supplemented by five additional network segments. We attempt to provide an "enterprise" appearance to the users of the network by running many operating system versions and multiple like services on various hardware architectures. The black segment contains the classroom student machines, "soft" server targets, and research workstations. "Soft" targets are computers that have a default operating system installation and configuration with no patches applied. The gold segment, separated from the black network by a router, consists of a few administrative machines, research workstations, and several "hard" targets. "Hard" targets are machines that are configured with the most recent patches and hardened using the NSA and SANS security checklists, among other techniques. Services similar to those in the black network are running with the exception of improved, more secure services where applicable.

The student workstations in the black network provide each student an access point into the IWAR network where each student gets to exercise administration responsibilities (see Figure 2). Each student workstation uses the commercially available VMware Workstation software package to create a virtual network, enabling students to perform all tasks necessary for network and system administration. [6] This Virtual IA Network (VIAN) allows the user to create one or more virtual machines that run within a secure

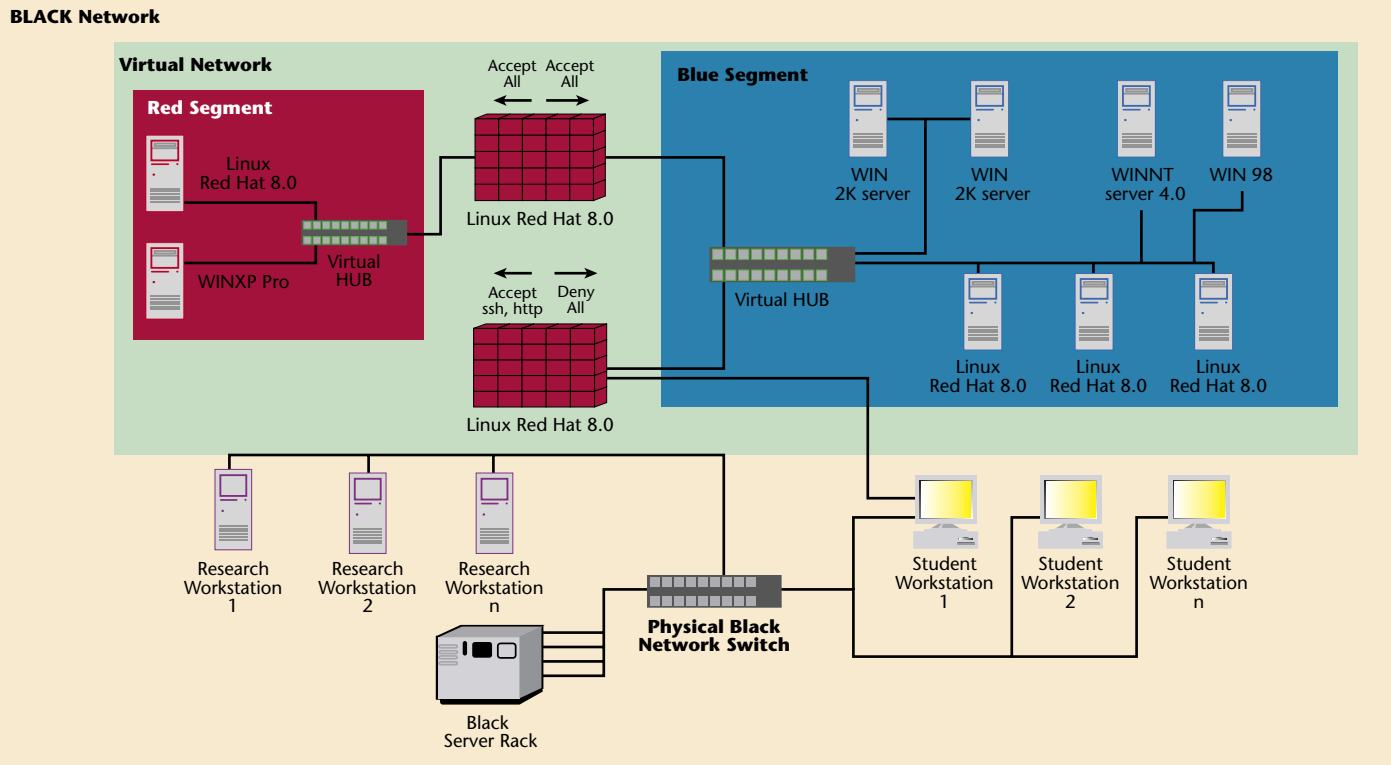


Figure 2. Student workstation with VIAN

boundary on a base operating system (OS). VMware runs on a host machine with Windows NT4, 2000, and XP, as well as Linux. The virtual machine (guest) OS can be any variant of Windows, DOS, or Linux. As many guest operating systems as disk memory allows can be loaded, and they can be run side by side if enough RAM is available on the host machine. The West Point implementation (P4 2.0 GHz with 1 GB RAM and a 30 GB hard disk) runs six virtual machines simultaneously with no significant latency problems.

For West Point's VIAN solution, the host operating system is Windows XP Professional. The virtual network is designed to present the user with two internal networks, a "red" network, containing machines that are used to launch exploits, and a "blue" network, consisting of target machines. These two networks are separated by a firewall (using Snort [7]) running on one of the Linux guest machines. A second firewall, also running on a Linux guest machine, acts as a gateway to the host machine. Each classroom workstation is configured to support two students. On the blue network, we have two separate installations of Windows 2000 server and Red Hat Linux 8.0 so each dedicated user of a computer has their own set of servers to administer. The Windows NT, Windows 98, and Red Hat 6.0 machines are target machines with no administrative requirements. There are also no administrative requirements for the red network, so it is shared by each user on a given workstation. This configuration gives each student a "virtual network" on their machine and provides some flexibility and creativity for the instructors and the students.

The virtual network is fully integrated into the lab and capable of reaching any machine on the IWAR network. The student can work to understand and fine-tune a given exploit or security tool in the virtual world without significant risk to the rest of the network. And then when the student is confident, he or she can use the new tool on the black or gold segments.

From a defensive perspective we use the virtual machines to demonstrate the concept of firewalls and system hardening. The Linux virtual machine running on the "external" network portion serves as the outside world from which the student wants to protect their internal network. These firewalls can be configured from a script or by student control. Students can launch network sniffers (such as Ethereal) on multiple systems to track packets through the network and observe where security policies are effective. The virtual machines also provide a hands-on laboratory where students install, configure, and then harden a group of operating systems using a security checklist such as checklists from SANS or the NSA. The virtual machines enable the student to perform these functions without tampering with the base operating system's configuration.

The VIAN in a student workstation offers many additional advantages over a typical laboratory configuration, such as—

- Additional guest systems or copies of an existing guest OS can be added by simply copying the VM folder. The number of guest operating systems that can exist on a given host is limited only by the amount of hard disk space.

- The guest OS is a full and complete installation of the operating system. All system calls and network protocol operations are executed exactly as if the guest OS was on its own hardware.

continued on page 28…

The laboratory development in the Information Technology and Operations Center is only one IT modernization success at USMA. The Information Technology and Operations Division (IETD), under the direction of Associate Dean COL Donald Welch, has also carved a path for the Academy toward building a fully integrated IT system that provides connectivity throughout the academic and barracks facilities.

West Point is both an academic institution and a military post, and therefore must maintain the free access to information normal to an academic environment while still meeting military information assurance standards. Because successful security requires outthinking the adversary information assurance is a very challenging subject in its own right, but equally important is the enthusiastic participation of the entire community. At West Point we have addressed both concerns with a single idea; we have formed an information assurance community of practice that includes both faculty and staff members. The result is a shared sense of ownership of network security and a much improved security posture, all without degrading the usefulness of the network.

According to Wenger, McDermott, and Snyder, communities of practice—

> *…are groups of people who share a concern, a set of problems, or a passion about a topic, and who deepen their knowledge and expertise in the area by interacting on an ongoing basis. [1]*

They don't just share abstract knowledge, but they work to solve real problems. In a well operating community of practice knowledge is shared, mentoring occurs, and real problems are solved. All members find value from the community whether they learn, teach, solve problems, or find solutions to their toughest problems. They are members because they believe they benefit from their participation. Communities of practice are outside of the normal organization of the institution. Members are not assigned positions by management—they gain their authority from the consensus of the members themselves. In a successful community of practice knowledge is what counts—sharing it, gaining it, and applying it.

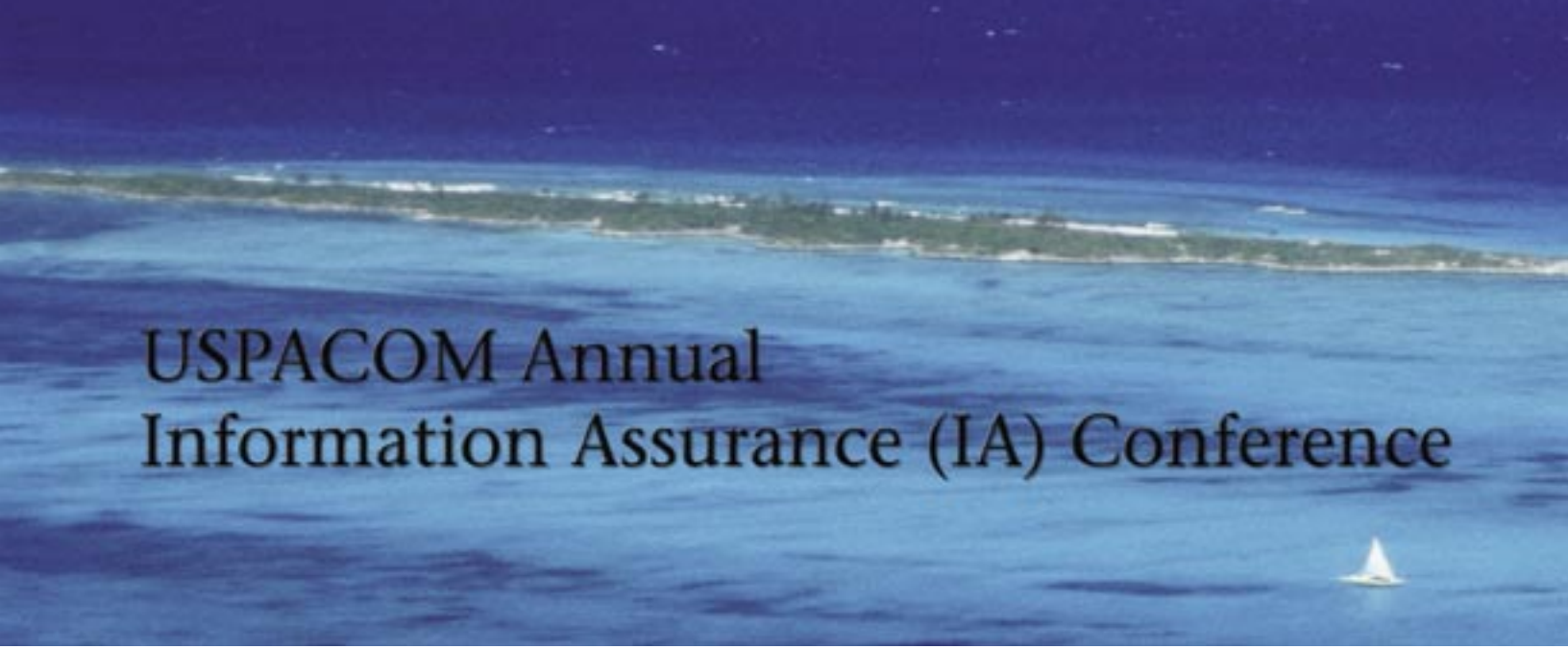
In information assurance the worst case adversary is a thinking, willful, and creative human being and not the elements of chance. This makes the field is very dynamic—as soon as defenders develop defenses, the attackers are at work on a way to defeat it. If there is a way past the network defense, the attackers will find it and exploit it. The network at a university is also indispensable its mission. The wrong security measures can be much more effective at denying the legitimate users access to the network resources than even a skilled attacker! Deciding how much risk to take, understanding the full ramifications of a security measure, keeping administrators and users educated and vigilant are all very difficult tasks for information technology leaders. The users tend look at security measures as impediments to accomplishing their mission. Security measures that the users don't understand or worse don't really make sense can be met with resistance that sometimes even crosses into defiance. An acceptable level of security cannot be achieved by fiat. For an effective defense, the network users must not circumvent security measures, must comply with the policies, and must go so far as to participate in the defense of the network.

West Point's community of practice is called its Computer Emergency Response Team (CERT). The West Point CERT is a community of practice rather than a committee because it is outside the hierarchy and participation is voluntary. People join and stay in communities of practice because they find value in the interactions. [2] The information technology field is a knowledge intensive field, so the opportunity to learn is a strong enticement to the information technology support people. There are many people at USMA that have expertise in computer network security. The Department of Electrical Engineering and Computer Science has a center focused on computer network security research. They bring familiarity and understanding of the current computer security literature to the CERT. There are experienced system administrators who bring years of experience securing networks, especially the West Point network to the CERT. Additionally, there are Army officers who have worked computer network security in other Army assignments and they bring that perspective to the CERT. All members have something to contribute and all have something to learn.

By taking this unique approach West Point has been able to develop some very good solutions to information assurance problems and build support for them by including experts from all parts of the command. The result has been a far better information assurance posture than before the CERT's creation. This exact model may not apply in all installations but communities of practice are powerful and should be considered in challenging domains like information assurance. ■

References

1. Wegner, Etienne, Richard McDermott, and William Snyder. Cultivating Communities of Practice. Boston: Harvard Business School Press, 2002.
2. Ibid.



USPACOM Annual Information Assurance (IA) Conference

by Harry Xenitelis

The Computer Network Defense (CND) and Information Assurance (IA) Directorate (J65) within the United States Pacific Command (USPACOM) recently hosted its 19th annual IA Conference in Honolulu, Hawaii on May 20–23, 2003. The conference drew nearly 300 participants from Europe to Korea and many places in between.

In the spirit of this year's theme, "Security Through Cooperation," USPACOM brought together IA representatives from nearly all the Combatant Commands and several Department of Defense (DoD) Agencies with Pacific Theater IA representatives from every Command, Service, and standing Joint Task Force (JTF). The overall goal of this year's conference was to share information and discuss topics ranging from the latest IA policies, trends, issues, solutions, how organizations are structured, operational lessons learned, and more. Keynote speakers for each day were Mr. Richard C. Schaeffer, IA Deputy Director (IA DDIR) for the National Security Agency (NSA); MG James D. Bryan, Vice Director, Defense Information Systems Agency (DISA)/Commander, Joint Task Force–Computer Network Operations (JTF–CNO); Mr. Robert Lentz, Director, ASD/NII, Director, IA; and Mr. Randall Cieslak, Chief Information Officer (CIO), USPACOM. The conference featured over 35 presentations related to CND, law enforcement, policies, programs, and information sharing at both the unclassified and classified levels.

The first day started with opening remarks by USPACOM's J6, COL(P) Randolph Strong and keynote speaker Mr. Richard C. Schaeffer, who provided key operational historical examples supporting DoD's need to evolve and the impact those changes will have on future technologies. Mr. Schaeffer discussed how the DoD is in the process of creating a paradigm-shift oriented towards network-centric warfare. The Secretary of Defense (SECDEF), Donald Rumsfeld, declared recently that more information sharing must be done via a secure network to provide both "actionable information" and "seamless joint coalition warfighting forces." He pointed out that early failed DoD attempts at implementing wireless technologies and how the DoD is most hindered at boundaries that exist between military and civilian infrastructures underscore the complexity of assembling the networks that will be used in the future. Implementing this new paradigm of network-centric warfare will be the challenge for DoD in coming decades.

On day two, keynote speaker MG James D. Bryan, who was one of the attendees at the first USPACOM IA conference, gave a powerful presentation on the immense impact technology has had on the daily lives of Americans, America's economy, and the dramatic increasing role in today and tomorrow's military. After articulating how critically important technology has become to both the civilian and military sectors of the United States, MG Bryan provided an overview of computer network threats and their impact on our networks over the past several years. He concluded his presentation by emphasizing the importance for all of us in the IA community to continue to work hard on the myriad of issues pertaining to IA in order to meet the needs of both the civilian and military sectors of this country.

Mr. Robert Lentz, keynote speaker for day three, informed the audience that the Office of the Secretary of Defense (OSD) is viewing IA from a high-level perspective and the impact and effects within DoD and worldwide. He provided an overview on how the Office of the Assistant Secretary of Defense (OASD) is reorganizing but stressed that his organization will remain directly under their current leadership and report directly to the SECDEF, who has been very involved with IA efforts. In fact, the SECDEF had challenged OSD to create a new IA Strategic Plan. Mr. Lentz stated that their plan includes five key goals—

1. Information protection
2. Defense of systems and information
3. Provision of situational awareness globally
4. Transformation and enabling IA capabilities
5. Empowerment of the workforce

Mr. Lentz provided details pertaining to each key goal and associated funding to accomplish the goals.

Day four's keynote speaker, Mr. Randall Cieslak, focused on one core problem prevalent today—deployment of many "information age" services throughout DoD with an "industrial age" mentality. To explain this dilemma, Mr. Cieslak used the example of how information system boundaries frequently exist within joint commands between different Services. He argued that Commands should be organized into communities, where individuals sharing similar missions and goals are grouped into information enclaves. He expressed how this "information age" paradigm focuses on proper organization of information so appropriate users within established communities would have the access they require. Mr. Cieslak then described in detail how this concept would be employed and its affect on network architecture. He concluded by stating that a truly robust global information grid (GIG) can be created by wrapping critical information in community enclaves and overlaying them on a secure network infrastructure.

A complete listing of conference speakers, conference agenda, presentations, and a more detailed 33-page conference overview can be found on USPACOM's SIPRNET Web site located at http://www2.hq.pacom.smil.mil/J6/J65 (click on the "2003 PACOM IA Conference" tab). ■

About the Author

Harry Xenitelis

Mr. Harry Xenitelis is an IA officer for Headquarters, USPACOM J653 Branch. His primary role is to serve as USPACOM's Tier 1 IA exercise planner.

Mr. Xenitelis has served in the U.S. Army for over 16 year as both an Active Duty and Reserve Signal Corps Officer. He has served in both conventional and special operations units while on Active Duty and currently augments the J6 Directorate at HQ SOCPAC as a Reservist.

Vulnerability Assessments

by Abraham T. Usher

Vulnerability assessments are an important part of an overall risk management plan for Information Assurance (IA) professionals. Given that most enterprise networks have hundreds or thousands of on-line systems, vulnerability analysis and assessment by manual methods is virtually impossible. Accordingly, software tools play an important role in enabling system and network administrators to perform vulnerability assessments on their networks. This article examines the types of vulnerability assessment tools available, how they work, and how these tools can be incorporated into a comprehensive security program.

Definitions

- **Vulnerability**—A weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system.
- **Vulnerability Analysis and Assessment**—A systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Types of vulnerability scanners

Vulnerability scanners fall into one of five main categories: host scanners, network scanners, web scanners, database scanners, and war-dialers.

- **Host based**—These tools may examine critical system files, active processes, file shares, and the configuration and patch level of a particular system. They generally produce the most detailed results of any scanner type because they run on the host system itself at the same permission level as the user running the scan. A disadvantage to host based scanners is that in some cases it is not easy to aggregate and correlate the results across several hosts (imagine an administrator trying to physically visit and test 1,000 workstations).
- **Network based**—In contrast to host-based scanners, these tools examine available network services for vulnerabilities through port status, banner grabbing, protocol compliance, service behavior, or exploitation (e.g., Nessus). [1]
- **Application (Web)**—These are a specialized form of network scanner that interrogate Web servers for known vulnerabilities (e.g., Nikto). These scanners often check for the presence of demonstration Web pages, insecure cgi-bin files, default accounts, form validation errors, directory traversal attacks, and other vulnerabilities.
- **Application (database)**—Also a specialized form of network scanner, these tools interrogate database servers for known vulnerabilities (e.g. ISS Database Scanner).
- **War-dialers**—Automate the process of scanning phone numbers looking for modems accepting incoming connections (e.g., PhoneSweep). Once they find a modem, they attempt to login. War-dialers are not covered in further detail in this article.

How network vulnerability scanners work

These products work by attempting to automate the first three steps of the same methodology that a hacker uses. First, a network footprint analysis is conducted by scanning for accessible hosts. As accessible hosts are identified, the tools enumerate available network services (e.g., FTP, SSH, HTTP, etc.) on each host. As part of the enumeration of services, scanners attempt to identify vulnerabilities

Hacker's methodology [2]

1. Perform a footprint analysis
2. Enumerate information
3. Obtain access through user manipulation
4. Escalate privileges
5. Gather additional passwords and secrets
6. Install backdoors
7. Leverage the compromised system

through port status, banner grabbing, protocol compliance, service behavior, or exploitation.

Banner grabbing refers to grabbing information that a network service broadcasts about itself. For example, opening a telnet session to a mail server might yield the message—

```
220 mailhost.company.com ESMTP service
(Netscape Messaging Server 4.15 Patch 7
(built Sep 11 2001)).
```

This example banner reveals that the specific type of mail server running and its patch level. Similarly, a telnet connection to a Web server might yield information like—

```
HTTP/1.1 200 OK
Date: Wed, 02 Jul 2003 22:03:21 GMT
Server: Apache/1.3.27 (Win32) PHP/4.2.2
X-Powered-By: PHP/4.2.1
Connection: close
Content-Type: text/html
```

In this case, the banner reveals the time on the Web server, the server type, and the operating system that it is running on.

Port status refers to checking to see which network ports are open to allow connections to applications. For network services that use Transmission Control Protocol (TCP), this is done by sending a TCP connect() request to ports on the remote system. If the queried port is listening, the connect() request will succeed. If the queried port is not listening, the connect() fails and the port is considered closed. There are several other methods of checking port status (TCP SYN scans, TCP FIN scans, etc.) that are beyond the scope of this article (see Figure 1 on page 26).

Protocol compliance refers to the way an application or operating system adheres to a standard procedure for data processing or transmission. One of the most common ways of using protocol compliance to identify remote systems is to interrogate the TCP stack. By monitoring the header information of outbound packets, it is possible to make accurate guesses on the remote operating system. By examining the Time To Live (TTL) on the packet, its Window Size, the Don't Fragment bit, and the Type of Service (TOS), it is possible in many cases to determine exactly which implementation of the TCP stack is on the remote system. Determining the TCP stack narrows the number of possible operating systems, sometimes identifying the exact operating system.

Service behavior refers to the way that a network service responds to remote requests. Different implementations of a given type of service may provide slightly different behavior from remote requests. For example, a "help" command response from a sendmail E-mail server is different than the result from a postfix E-mail server.

Once a scanner finds a host with open ports, it will check those ports for vulnerabilities to known attacks. Most scanners include exploit tests that verify whether or not a given service or application is vulnerable. Scanning tools perform their tests based on their database of vulnerabilities. If a vulnerability is not included in a tool's database, then it cannot be detected by scanning. Just as anti-virus products must be constantly updated with new signatures, assessment tools must be continually updated with revisions to their vulnerability databases.

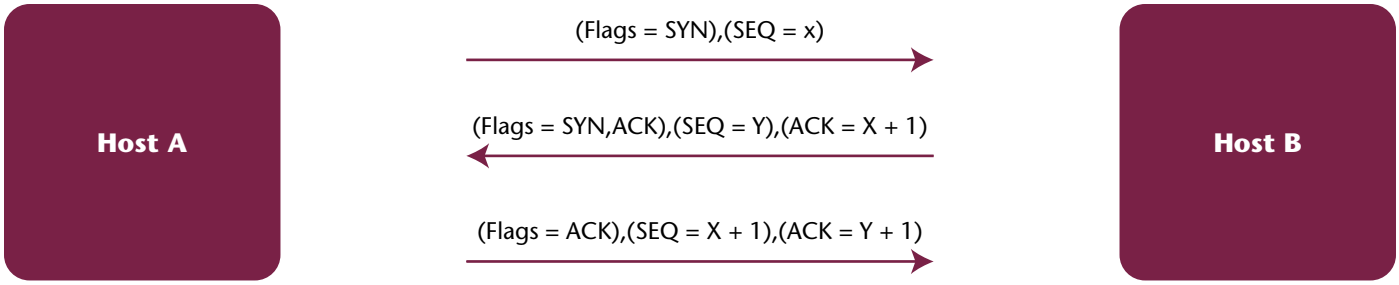


Figure 1. TCP connection (3-way handshake)

How vulnerability scanners can be incorporated into a security plan

Scanning tools can be an invaluable asset for obtaining a "snap-shot" of the vulnerabilities that exist on a network at a given point in time. Most tools include reporting tools that explain the vulnerabilities detected and provide a ranking of the criticality of each problem (high, medium, low, etc.). For enhanced effectiveness, assessments should be performing on a routine basis. Most users and administrators would not have confidence that a host is free from malicious code if an anti-virus scan was only performed on it once a year. In a similar manner, networks must be checked periodically for risks due to new hosts being connected or newly discovered weaknesses in existing applications and operating systems.

Identifying vulnerabilities on a system or network is only half of the challenge—the other half is actually fixing the problems found through patching, updating, or re-configuring. System and network administrators must schedule time to fix the problems discovered as a result of vulnerability assessments or else the assessments have no value in improving security.

Unfortunately, scanning tools suffer from false positive problems and false negative problems similar to anti-virus products. "False positives" refer to when a tool finds a vulnerability that does not exist. For example, a particular scanner may report that a network server is a Windows 2000 system that is vulnerable to a known Microsoft Internet Information Server (IIS) Web server bug, when in fact the server is a Linux system running the Apache Web server. [3] "False negatives" refer to when a tool fails to find an existing vulnerability. An example of this behavior could be when a particular tool tests a network host and fails to discover that it is remotely exploitable through an anonymous login. [4]

Common sense must be applied to all findings to ensure meaningful vulnerabilities are fixed, while at the same time no time is wasted on erroneous findings. One strategy for reducing the number of false positives and false negatives is to run two different scanners against a given network and compare the results. In most cases, the results of both tools will compliment one another so that no weaknesses slip through the cracks.

Conclusion

Vulnerability analysis and assessment tools provide a useful mechanism for auditing the configuration and security of systems within a network. They provide a semi-automated way for administrators to discover security "holes" that need to be plugged up before crackers or malicious code exploit them. As with all information technology products, vulnerability analysis and assessment tools are not perfect. Sometimes they yield false positives (causing extra work for administrators), other times they result in false negatives (leading to a false sense of security). However, as part of a comprehensive security strategy, these tools can provide a very useful mechanism for reducing risk. ■

About the Author

Abraham T. Usher

Mr. Usher is Deputy Director of the Information Assurance Technology Analysis Center (IATAC). He graduated from the U.S. Military Academy in 1996 with a B.S. double major in Modern Standard Arabic and German language studies and a minor in Computer Science.

References and Resources

1. As described by Adam Shostack's briefing entitled "Towards a Taxonomy of Vulnerability Scanning Techniques."
2. As defined by Eric Schultze in his article "Thinking like a hacker" http://www.shavlik.com/Whitepapers/Thinking%20like%20a%20hacker.doc.pdf.
3. As describe in the SANS/FBI Top 20 list at http://www.sans.org/top20/#W1.
4. As described in the SANS/FBI Top 20 List at http://www.sans.org/top20/#W5.

MITRE Common Vulnerabilities and Exposures (CVE) list http://www.cve.mitre.org/

Remote OS Detection via TCP/IP Fingerprinting http://www.insecure.org/nmap/nmap-fingerprinting-article.html

What is p0f (Passive OS Fingerprinting) and what does it do? http://www.sans.org/resources/idfaq/p0f.php

Nessus http://www.nessus.org

Towards a Taxonomy of Network Security Assessment Techniques http://razor.bindview.com/publish/papers/taxonomy.html#_Toc474211193

by JOSN Melissa Pinsonneault

Virginia Beach, Virginia…

In May 2002, the Chief of Naval Operations (CNO) released NAVOP 007–02 establishing Information Operations (IO) as a major warfare area, on par with other major warfare areas (AAW, ASW, ASUW). CNO called for the establishment of general and specialized training in IO because it will continue to play a major role in the Global War on Terrorism (GWOT).

Commander Naval Network Warfare Command (NETWARCOM) was established July 11, 2002, with Vice Admiral Richard Mayo as the first commander. The command serves as the U.S. Navy's central operational authority for space, information, technology requirements, network, and IO in support of naval forces afloat and ashore. One of VADM Mayo's first actions was to stand up a training working group comprised of members of Commander Fleet Forces Command, numbered fleet and battle group staffs from the Atlantic, European, and Pacific theaters, Fleet Information Warfare Center (FIWC), and the naval training community to assess the status of IO training throughout the fleet. This working group determined that no single, comprehensive naval IO course existed, nor did any substantive IO training exist for those personnel being sent to perform IO duties, and that failure to develop a training opportunity to fill this gap would result in a continued crucial shortfall in a critical warfare mission area within the fleet. Using CNO and Naval Education and Training Command (NETC) guidelines for task analysis, the working group determined which skills and knowledge factors were required to function as IO professionals at the operational and tactical command levels.

In December of 2002, a curriculum development team was established leveraging subject matter experts from various Fleet IO cells and curriculum development expertise from the NETC organization. This team was given the task of turning the list of required skills and knowledge factors developed by the IO training working group into a human performance solution, in this case, an instructor led course

continued on page 29…

When students from the class were asked for comments about how they felt the course will prepare them for their IO assignments, they responded—

An aggressive, extensive course encompassing operational aspects of IO from planning to execution for application in a joint or naval environment.

LCDR Kim Cobb
COMPACFLT Det IRC
San Diego, California

A comprehensive program for Marines to master IO at the tactical and operational level.

LtCol Neal McCarthey, USMC
U.S. Strategic Command (USSTRATCOM)
Omaha, Nebraska

The practical exercises forced me to translate the theoretical concepts of IO into tools the IWC will use to support the Battlegroup Commander.

CDR Al Camp
IW Commander, Carrier Group Eight
Norfolk, Virginia

NIWSOC hits the target. It's the first IO course I've seen that competently ties strategic guidance to operational and tactical execution.

LT Fred Stratton
Center for Cryptology
Pensacola, Florida

…continued from page 21

- If an exploit or a configuration change causes significant damage to a guest OS, it can simply be deleted and copied back from an archive location.
- Any damage or intentional changes made in the previous session are discarded when the machine ends its session, and the guest OS is rebooted.
- A user is able to exercise complete administrative control over a group of machines and network components. The ability to operate as an administrator provides an invaluable hands-on learning experience.
- The virtual network can operate in isolation or can interact with external networks.
- The VIAN can provide a highly mobile solution by implementing it on a laptop.

In addition to the black and gold subnets, the IA network also contains a subnet dedicated to Honeynet research. The West Point Honeynet Project (WPHP), an affiliate of the Honeynet Project, uses a network within the IWAR lab to prototype emerging Honeynet technologies. Honeynets are networks built for the sole purpose of attracting "hacker" type traffic for intrusion detection and methodology analysis.

The IWAR is also supported by the Searchbox network, a commercial broadband access point that enables faculty and cadets to conduct research on the Internet without the potential of compromising the academy network or violating network policies. In addition to researching topics, this solution provides a network connection for our research, training, and education on forensics analysis. [7] The Searchbox network is routed thought a wireless access point allowing connectivity throughout the lab using a group of laptops and wireless technology research.

The third IWAR subnet, the SIGSAC network, supports USMA's Special Interest Group for Security, Auditing, and Control (SIGSAC). Designed and built in 2002 by members of SIGSAC, the network, otherwise known as the SIGSAC "clubhouse" supports the group of over 300 members by providing an isolated network of computers from which members of the club may learn and explore both offensive and defensive tools used in cyber warfare. The advantages to having a network specifically set aside for our SIGSAC club is that it allows them to experiment with offensive and defensive tools, again, in an isolated network without the concern of interfering with our IA classes. Since the individuals using the SIGSAC network are generally less experienced, they work on a smaller network separate from the IA network, minimizing the risk due to a mistake and minimizing the time to rebuild.

The modular design of four separate networks provides us with the flexibility to combine networks, if we determine it would be beneficial in the future. Domain names and IP addresses were carefully chosen so as not to have conflicting namespace issues. If for example, we decide to create a mini-Cyber Defense exercise [8] with our SIGSAC club members, we could combine the SIGSAC network and other portions of the IA network (for example the gold network) through either a CAT–V cable or wireless connection. The design of the IWAR laboratory's networks tried to anticipate such future requirements.

The IWAR lab and classroom provides a robust environment where users can see and experience first hand topics from IA basics to more advanced topics. Additionally, incorporating the VIAN solution, the network can be modified to closely mirror a production system. This allows administrators to experiment with various topologies and security configurations and policies prior to deployment. ■

About the Authors

MAJ Ronald C. Dodge, Jr., Ph.D., USA

MAJ Ronald C. Dodge, Jr. is an Aviation officer and a member of the Army Acquisition Corps. His military assignments include Aero Scout Platoon Leader, Battalion Assistant S3, and Brigade Assistant S1 in the 7th ID(L), Fort Ord; Company Aviation Maintenance Officer and Battalion S4, 17th Aviation BDE, Korea; and AVIM Company Commander and Battalion S4, 12th Aviation Battalion, Davison Army Airfield.

His current assignment is Assistant Professor and Senior Research Scientist in the Information Technology and Operations Center (ITOC) at the U.S. Military Academy.

MAJ Dodge graduated from Central Valley High School, Spokane Washington, in 1983. He received his Bachelor of Arts in Computer Science and Economics from University of Colorado, Boulder in 1987; his Masters of Science in Computer Science from George Mason University in 1998; and his Ph.D. in Computer Science from George Mason University in 2001. His military education includes Initial Entry Rotary Wing School, Maintenance Test Pilot School, the Combined Arms Services Staff College, and the Command and General Staff College.

MAJ Dodge's awards include the AAM, ARCOM(2), MSM, and Air Medal.

LTC Daniel Ragsdale, Ph.D., USA

LTC Ragsdale has nearly twenty-two years of active military service. He was commissioned a Second Lieutenant of Infantry upon graduation from the U.S. Military Academy in 1981. During his Army career, LTC Ragsdale has served in a variety of important operational, and research and development assignments.

His current assignment is Associate Professor and Director of the Information Technology and Operations Center (ITOC) at the U.S. Military Academy.

During his military career, LTC Ragsdale has participated in two significant contingency operations. First, in 1983 he took part in Operation Urgent Fury in Grenada, serving as platoon leader in the 2nd Battalion 505th Infantry, 82nd Airborne Division. Later, in 2002 LTC Ragsdale participated in Operation Enduring Freedom in Afghanistan, serving as the Chief of Assessment for the Combine and Joint Task Force (CJTF–180).

His military awards include: the Meritorious Service Medal with 3 Oak Leaf Clusters, the Joint Service Commendation Medal, the Army Commendation Medal,

the Army Achievement Medal with 3 Oak Leaf Clusters, and the Combat Infantryman Badge.

LTC Ragsdale received his Bachelor of Science from the U.S. Military Academy in 1981, his Masters of Science in Computer Science from the Naval Postgraduate School in 1990, and his Ph.D. in Computer Science from Texas A&M in 2001.

COL Donald J. Welch, USA

COL Donald J. Welch was commissioned a Second Lieutenant of Infantry in 1979 upon graduation from West Point. He served over four years in Hawaii as a platoon leader, executive officer, brigade assistant operations officer, and company commander. He attended the Canadian Land Forces Staff Course at Fort Frontenac, Kingston, Ontario.

He received a Masters Degree in Computer Science from the California Polytechnic State University in 1987 prior to his assignment as Instructor, Assistant Professor, and Research Officer at the Department of Geography and Computer Science, West Point from 1987–1989 and in the Department of Electrical Engineering and Computer Science in 1990.

After attending the Command and General Staff College at Fort Leavenworth, Kansas, he was reassigned to the National Capitol Region, where he was the assignment officer for all Computer Specialist Officers in the U.S. Army. He then joined Delta Force in Fort Bragg, North Carolina, integrating information technology into special missions.

He then attended the University of Maryland and earned a Ph.D. in Computer Science in 1998. He assumed duties as Academy Professor in the Department of Electrical Engineering and Computer Science where he headed the Computer Support Group and founded the Fundamentals Program. He was reassigned to his current position as Associate Dean for Information and Educational Technology in 2000, but retains teaching duties. COL Welch's current research is in IA and IA education.

References

1. United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, P.L. 107-56, Title X, Section 1016.
2. President's National Strategy to Secure Cyberspace, Feb 10, 2003, http://www.educause.edu/security/national-strategy
3. J. E. Stice, "Using Kolb's Learning Cycle To Improve Student Learning", Engineering Education, February 1987, pp. 291-296.
4. C. E. Kaucher and J. H. Saunders, "Building an information assurance laboratory for graduate-level education," presented at 6th National Colloquium for Information System Security Education, Redmond, WA, 2002.
5. J. Schafer, D. J. Ragsdale , J. R. Surdu, and C. A. Carver, "The IWAR range: a laboratory for undergraduate information assurance education," presented at Consortium for Computing in Small Colleges, Middlebury, Vermont, 2001.
6. VMware, www.vmware.com, VMware Workstation 3.0 User's Manual, 2001.
7. The Honeynet Project, Know Your Enemy Revealing the Security Tools, Tactics, and Motives of the Blackhat Community. Boston: Addison-Wesley, 2002.
8. D. W. Welch, D. J. Ragsdale, and W. Schepens, "Training for Information Assurance," IEEE Computer, pp. 2-9, 2002.

…continued from page 27

"NETWARCOM"

of instruction. That solution is the Naval Information Warfare Staff and Operations Course (NIWSOC).

NIWSOC is designed to prepare personnel ordered to IO assignments on a Naval Component, Afloat, or Shore Staff. It is also suitable for individuals involved in IO as Naval representatives assigned to the Department of Defense (DoD) or other U.S. Government agencies or Service component headquarters. NIWSOC provides students with the fundamental knowledge and skills necessary to conduct naval IO, emphasizing practical application and recent experiences that may be applied to current challenges. Topics include—

- Core elements and supporting activities of IO
- IO policy, doctrine, and organization
- IO capabilities and related activities
- IO planning and targeting
- Naval-specific considerations

Students are required to demonstrate their learning by successfully completing an end of course examination and through participation in comprehensive practical exercises that are integrated throughout the course.

The pilot course for NIWSOC convened March 26, 2003 and graduated April 10, 2003 with a class make up drawn from a broad spectrum of IO experience ranging from an Ensign with no experience what so ever to a USMC LtCol with several years experience as an IO staff planner. The next NIWSOC is scheduled to convene August 11–22 and will be offered every two months with the February 2004 course to be conducted in San Diego, California. The complete course schedule can be found at http://ekm.netwarcom.navy.smil.mil/n92/NIWOSC.htm. ■

About the Author

JOSN Melissa Pinsonneault

JOSN Melissa Pinsonneault is a U.S. Navy journalist assigned to the Naval Amphibious Base Little Creek, Virginia Beach, Virginia.

IATAC Conference, Meeting, & Event Planning

Providing technical and administrative support for scientific, technical, and DoD-related information assurance management conferences, symposia, workshops, and other meetings. We will coordinate all resources to ensure your event is a success!

Services

Pre-Event Support

- Site selection
- Catering arrangements
- Contract negotiation
- Promotion and marketing
- Event support materials
  - Agenda
  - Notebooks and folders
  - Presentation materials
- Security and registration

On-Site Support

- Coordination with caterers
- Check-in of registrants
- Document control
- Security problem resolution (if required)

Post-Event Support

- Create and assemble event proceedings
  - CD-ROMs
  - Hard copies
- Distribute event proceedings
- Generate final report

Benefits

A Proven Approach

- Detailed pre-planning expertise
- History of numerous successfully planned and executed events
- Expertise in policy adherence for conducting classified conferences
- Commitment to sponsor needs

Hotel/Sales/Catering

We work closely with hotels to block rooms and negotiate a predetermined conference room rate, coordinate food and beverages for breaks, lunches, and receptions.

Attendees

We work closely with each attendee to ensure we have all the appropriate registration information, security forms, and fees.

Event Marketing

We identify and take advantage of all appropriate promotional and marketing opportunities with professional associations, newsletters, other periodicals, and Web sites.

IATAC possesses world-class telecommunication, graphics, printing, and reproduction capabilities, providing service and support to guarantee the highest quality conference preparation materials, brochures, posters, presentations, proceedings, and product displays, both electronic and hard copy. IATAC also possesses outstanding multimedia presentation capabilities, which includes Web page development and on-line registration.

Classified Session Facilities

We coordinate with the appropriate personnel, ensuring compliance to classified event procedures. We work closely with security personnel and to develop appropriate mailing and storage instructions for classified presentations.

Please contact us at the information below.

3190 Fairview Park Drive, Falls Church, VA 22042

Commercial: 703/289-5454
STU–III: 703/289-5462
Fax: 703/289-5467
E-mail: iatac@dtic.mil
URL: http://iac.dtic.mil/iatac

Conference/Event Planner
April Perera
703/289-5699
iatac@dtic.mil

Promotional Director
Christina P. McNemar
703/289-5464
iatac@dtic.mil

product order form

Instructions: All IATAC **LIMITED DISTRIBUTION** reports are distributed through DTIC. If you are not a registered DTIC user, you must do so **prior** to ordering any IATAC products (unless you are DoD or Government personnel). **To register On-line:** http://www.dtic.mil/dtic/regprocess.html.
The *IAnewsletter* is **UNLIMITED DISTRIBUTION** and may be requested directly from IATAC.

Name _____ DTIC User Code _____

Organization _____ Ofc. Symbol _____

Address _____ Phone _____

_____ E-mail _____

_____ Fax _____

Please check one: ❑ USA ❑ USMC ❑ USN ❑ USAF ❑ DoD
❑ Industry ❑ Academia ❑ Gov't ❑ Other

Please list the Government Program(s)/Project(s) that the product(s) will be used to support: _____

_____

LIMITED DISTRIBUTION

IA Tools Reports (softcopy only)

❑ Firewalls ❑ Intrusion Detection ❑ Vulnerability Analysis

Critical Review and Technology Assessment (CR/TA) Reports

❑ Biometrics (soft copy only) ❑ Computer Forensics* (soft copy only) ❑ Configuration Management
❑ Defense in Depth (soft copy only) ❑ Data Mining ❑ Exploring Biotechnology
❑ IA Metrics ❑ Network Centric Warfare
❑ Wireless Wide Area Network (WWAN) Security

State-of-the-Art Reports (SOARs)

❑ Data Embedding for IA (soft copy only) ❑ IO/IA Visualization Technologies
❑ Modeling & Simulation for IA ❑ Malicious Code

* You MUST supply your DTIC user code before these reports will be shipped to you.

UNLIMITED DISTRIBUTION

Hardcopy *IAnewsletters* available

Volumes 4		❑ No. 2	❑ No. 3	❑ No. 4
Volumes 5	❑ No. 1	❑ No. 2	❑ No. 3	❑ No. 4
Volumes 6	❑ No. 1	❑ No. 2		

Softcopy *IAnewsletters* back issues are available for download at http://iac.dtic.mil/iatac/news_events/ia_newsletter.htm

Fax completed form to IATAC at 703/289-5467

September

e-Gov Enterprise Architecture Conference
September 10–12, 2003
Ronald Reagan Building and International Trade Center, Washington, DC
jcalore@fcw.com

Management of Knowledge Intensive Dynamic Systems (MKIDS) 2003
September 15–17, 2003
BWI Airport Marriott, Linthicum, Maryland
http://www.iaevents.com/MKIDS03/NewInfor.cfm

Information Assurance
September 15–17, 2003
Ronald Reagan Building and International Trade Center, Washington, DC
http://www.e-gov.com/events/2003/ia/

C4IEWS Path to Transformation and Homeland Security
September 15–19, 2003
Atlantic City Convention Center, New Jersey
http://www.afcea-ftmonmouth.org/MTHS_2003/Homeland_Index.html

ASNE Symposium "Harnessing the Power of Technology for the Warfighter"
September 16–18, 2003
Convention Center, Bloomington, Indiana
http://www.crane.navy.mil/asnesymposium03/

U.S. Army DOIM Conference
September 29 - October 3, 2003
Hyatt Regency Hotel, Atlanta, Georgia
http://www.afcea.org/doim2003/

InfowarCon 2003
September 30 - October 3, 2003
Renaissance Hotel, Washington, DC
http://www.infowarcon.com

October

National Summit on Security
October 1–2, 2003
Washington Convention Center, Washington, DC
http://www.NationalSummitonSecurity.com

21st C4IST Conference
October 7–9, 2003
Fort Huachuca, Arizona
http://www.laser-options.com/afcea/

Interoperability
October 14–16, 2003
Doubletree Hotel, Crystal City, Virginia
http://www.idga.org/cgi-bin/templates/10578656667824096679670001/genevent.html?topic=196&event=3418

9th Annual Biometrics Summit 2003
October 15–17, 2003
Las Vegas, Nevada
http://www.aliconferences.com

AFCEA's 24th TECHNET Europe "Internet: Friend or Foe?"
October 16–17, 2003
Jolly Midas Hotel, Rome, Italy
http://www.technet-europe.com/

FIAC 2003
October 21–23, 2003
University of Maryland University College, Inn and Conference Center, Adelphi, Maryland
http://204.168.24.134/event.asp?eventid=1508

Workshop on Rapid Malcode (WORM)
October 27, 2003
Wyndham City Center, Washington DC
http://pisa.ucsd.edu/worm03/

November

Public Key Enabling (PKE) Technical Working Group
November 17–21, 2003
Orlando World Center Marriott, Orlando, Florida
http://www.iaevents.com/PKE03.2/newinfo.cfm

TechNet Asia-Pacific 2003 "IT: Breaking the Distance Barrier, Sea-Land-Air-Space"
November 4–6, 2003
Sheraton Waikiki and Royal Hawaiian Hotels, Honolulu, Hawaii
http://www.afcea.org/asiapacific2003/default.asp

National Threat Symposium and Security Awareness Fair
November 19–20, 2003
Johns Hopkins University Applied Physics Laboratory, Laurel, Maryland
http://www.iaevents.com

Global Milsatcom 2003
November 24–25, 2003
Radisson Portman Hotel, London, United Kingdom.
http://www.smi-online.co.uk/events/overview.asp?is=1&id=1444

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church, VA 22042

To change, add, or delete your mailing or E-mail address (soft-copy receipt), please contact us at the address above or call us at: 703/289-5454, fax us at: 703/289-5467, or send us a message at: iatac@dtic.mil