The
ITEA Journal
of Test and Evaluation
June/July 2004
Volume 25, Number 2
"INFORMATION ASSURANCE"

TECHNICAL PAPER ABSTRACTS:

Closing the Loop: Assessing Information Assurance and Interoperability in Operational Environments

David Aland
Advanced Information Engineering Services, Inc., Aeronautics, Arlington, Virginia

The essential attributes of information assurance (IA) for defense information systems are seldom well understood by system users and, consequently, are incompletely expressed in system requirements documentation. As a result, systems are often acquired and fielded that, while having been certified in relative isolation for security, have not been examined either for the full and necessary IA functionality, or in the appropriate operational context. Subsequent to fielding, re-assessment of these systems, which may have been altered during operational network integration, or perhaps operated in a fashion that differs from design, is too frequently anecdotal and not sufficiently rigorous to support analysis and follow-on upgrades and revisions. There is more than adequate policy regarding the inclusion of security and interoperability into information systems design, but there are inadequate data supporting the risk assessment and trade-offs that must be made with every fielded system. The missing element in a life cycle approach to IA assessment is a deliberate feedback loop that allows system developers and sponsors to review what technological approaches have been successful or not, and to review how they functioned. Such data would better serve a "spiral" development cycle that seeks to capture and institute innovations, and continually improve and adjust fielded systems to meet the changing operational environment.

Understanding and Evaluating Information Assurance

Peter H. Christensen
Marine Corps Operational Test and Evaluation Activity (MCOTEA), Quantico, Virginia

Information assurance (IA) is critical to the future of U.S. military operations. This paper addresses a number of interdependent systems characteristics that must be evaluated collectively to ensure fully effective IA. These characteristics include interoperability, IA, security certification and accreditation, electromagnetic environmental effects and spectrum management. Information is a key element of force transformation and network-centric warfare, and a Common IA Methodologies Working Group has developed standard issues, criteria and measures both for IA and its interdependent system characteristics. In an effort to position acquisition programs for success, capabilities developers and processes must be proactive in specifying IA requirements. Operational Test Agencies can aid this endeavor by addressing these critical characteristics in Test and Evaluation Master Plans. By planning ahead, the tasks of measuring and evaluating IA become relatively simple.

continued…

An Information Assurance Lesson Learned

Jim Cornell
Advanced Technology and Information Systems Branch,
Defense Information Systems Agency's Joint Interoperability Test Command
Washington Operations Division, Indian Head, Maryland

As technology races forward, intrusion detection and prevention systems improve. Generally, attacks launched against networks are well thought out, and the results can be difficult or impossible to detect while they are happening,and even harder to trace after the attack. To protect against such attacks, it is important for the test community to fully document the attacks, as well as the solutions formulated through troubleshooting.

Improving Information Assurance and Computer Network Defense Capabilities via COCOM Exercises

Peter W. Morel and LTC Jeffery Ballmer, USA
U.S. Army Test and Evaluation Command (ATEC),
Aberdeen Proving Ground, Maryland

More than seven years ago, the U.S. Department of Defense (DoD) embarked on a path to demonstrate that advanced information technologies hold the greatest promise of delivering revolutionary advances in force effectiveness. The key to this effort is achieving information superiority via a network-enhanced common operating picture that demands information systems that are vertically and horizontally integrated from the strategic to the tactical level. Development and procurement of these systems continues at a rapid pace. However, new systems introduce new vulnerabilities; likewise, potential adversaries are becoming increasingly adept at discovering and exploiting vulnerabilities of fielded systems. Assuring the integrity of the information and the security of the systems has become increasingly more challenging.

U.S. Air Force Information Assurance Computer Security System Vulnerability Assessment Process

Daniel D. Arredondo
92nd Information Warfare Aggressor Squadron, Air Force Information
Warfare Center, Lackland Air Force Base, San Antonio, Texas

To meet the ever-increasing threat of computer attacks on all Department of Defense systems, the U.S. Air Force has developed, through years of experience, procedures to help deny such attacks. The 92nd Information Warfare Aggressor Squadron (92 IWAS), Systems Vulnerabilities Flight, is in the day-to-day business of protecting all Air Force computer systems,encompassing those for ground, air, ship, space and homeland defense. The 92 IWAS mission statement calls for conducting opposing force information warfare operations and information warfare vulnerability assessments by replicating threat capabilities and tactics. This paper examines the following 92 IWAS capabilities: information assurance, leading-edge security tactics, exercise support and system vulnerabilities assessments.Each one of these functions is equally weighted in providing the customer with the best possible service available.

continued…

Operational Test & Evaluation: Another Approach to Validation of Models and Simulations

Rick Nunes-Vaz[1]
Land Operations Division,
Defence Science and Technology Organisation,
Edinburgh, South Australia

This paper examines the concepts of fidelity and validity in relation to modeling and simulation and, in so doing, exposes inadequacies and inconsistencies in current thinking about methods for assessing "fitness for purpose." It is argued in this paper that operational test and evaluation methods offer an alternate, promising approach by which to assess the validity of models or simulations, and that such an approach is more in keeping with the literature (Code of Best Practice in Experimentation,2002) *on the role of models and simulations in experimentation.*

Recent Association activity reminds me of a popular British series on public television that takes the viewer back in time to develop a thread or series of linkages to describe how things came to be that are routinely accepted in our world today. The central theme of the popular show is that everything has an explanation for how it has come to be, and that it is all driven by change. Change is a phenomenon that, like it or not, we must deal with on a daily basis; it is inescapable and persistent. Change can be an obstacle or it can be your friend. As the well-known and often-quoted Machiavelli said in *The Prince* (1532), "There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things."

What do Machiavelli's insights on change have to do with the conduct of the business of ITEA? Well, from my perspective as your Association President, a good deal. Changes to our Association have been frequent, challenging and profound. We have seen a number of changes that have added significantly to the Association's ability to better serve you, our members, while others have been less obvious but still important. Our Association leadership has embraced change and sees it as the agent for progress.

For example, we have implemented an Internet-based tool that allows attendees to now register on-line for the various workshops and symposia sponsored by ITEA's National Headquarters. This tool has been a huge success and is the first step in our quest to add other on-line features that will better serve our members. These on-line services include membership renewals and other routine business functions. Also, through a series of excellent off-site meetings, selected members of the ITEA Board of Directors,along with other key supporters, have crafted a number of initiatives to explore our Association's goals and objectives, business processes, means of outreach and communications, and membership services. Our goal is to clearly define what changes are required to better prepare us for the future.

The Association has also changed its approach to the conduct of workshops and symposia. We now look for opportunities to partner with other associations and organizations, co-sponsoring events such as the Directed Energy Professional Society's workshop and the Army Test and Evaluation (T&E) Days symposium,to offer programs that are more compelling to the broader T&E community.

ITEA's chapters are also dealing with change. Turnover of key officers, recruiting of new members, as well as the hosting of workshops and conferences, are but a few of the challenges that our chapters routinely confront. It is clear that change is all about us; however, I contend that change is our friend and gives us an opportunity to better serve you—our members—and to meet your needs as we move forward.

Gary L. Bridgewater

One change that I want to highlight is the retirement of Mr. Norm Haack, Assistant Director of ITEA National Headquarters, as of June 30. The entire T&E community knows Norm well and has appreciated the dedication and tireless efforts he has exhibited in building an outstanding educational program for the Association, in addition to the solid support he has provided to all of our members and chapters over the past six years. Norm has been the spearhead for developing ITEA's short course and tutorial program,which has not only provided the T&E community with professional education and training, but has also contributed to the overall financial success of ITEA. Norm is recognized by the whole T&E community as a consummate professional and an invaluable member of the Association's National Headquarters staff. We will miss Norm, but we wish him all the best in his retirement.

The good news is that change continues to be our friend in that Ms. Eileen Redd will succeed Norm as ITEA Assistant Director. Eileen is also well-known in the T&E community through her unwavering support in the planning and conduct of a number of ITEA national symposia, workshops and conferences. Eileen brings a great set of credentials to the Association, and she will continue to provide the great service to our membership that Norm has so admirably displayed.

Change moves us along. Washington Irving, in his *Tales of a Traveler* (1824), says it best when he states, "There is a certain relief in change, even though it be from bad to worse; as I have found in traveling in a stagecoach,that it is often a comfort to shift one's position and be bruised in a new place."

Gary Bridgewater

Threats and Leverage Possibilities for the Future

ADM William O. Studeman, USN (Ret.)
Northrop Grumman Mission Systems, Reston, Virginia

Successful information assurance requires robust test and evaluation (T&E) capabilities that are broadly competent and strategic in outlook. While this has always been important, it is even more compelling in the context of contemporary threats to our information technology (IT) and communications systems.

Because of these growing threats, two types of T&E are underway today. The first type is performed by engineers, developers, programmers and security professionals in an attempt to ensure that there are no product defects. The second type is conducted by malicious hackers and would-be intruders who are attempting to find and exploit undocumented vulnerabilities. This constant testing and probing by hackers is an unfortunate fact of life in a networked age. It underscores the critical importance of T&E and suggests the need for involvement of testers at earlier stages in the development process.

ADM William O. Studeman, USN (Ret.)

The threats

As it has always been, threats to our information systems come from insiders *and* outsiders. Despite the aggressive pursuit of technology solutions and processes, external attackers continue to penetrate our defense, federal, public and private IT and communications systems, and solutions for insider threats are even more challenging. While daily threats continue, more dire threats could be reserved for conflict. At one level, threats relate to unauthorized accessing, extracting or contaminating information. At another level, they have capabilities to deny access, take control or bring down entire IT systems and associated networks on obvious and non-obvious bases. Global and domestic hackers abound; disaffected employees (and possibly foreign agents) with access exist, and hostile nation-states and threat groups have theoretical capabilities to wage information warfare on a nation that is utterly dependent upon IT and communications systems to conduct virtually all that it does.

As we move to system-of-system, "enterprise"-type architectures, the complex interrelationships between systems create new vulnerabilities and new challenges for designers and testers. Ultimately, our national critical infrastructures, as well as our private/personal and workplace IT services, are threatened by critical vulnerabilities that are left unaddressed in the game of spiraling offense-defense interaction.

Threats discussed at a recent RSA Data Security, Inc., conference are instructive. Hackers seem clearly excited about the possibility that not only can they exploit holes in systems, but they can also exploit the hole-patching process by analyzing and developing worms for the patch before it is fully deployed (see *Figure 1*).

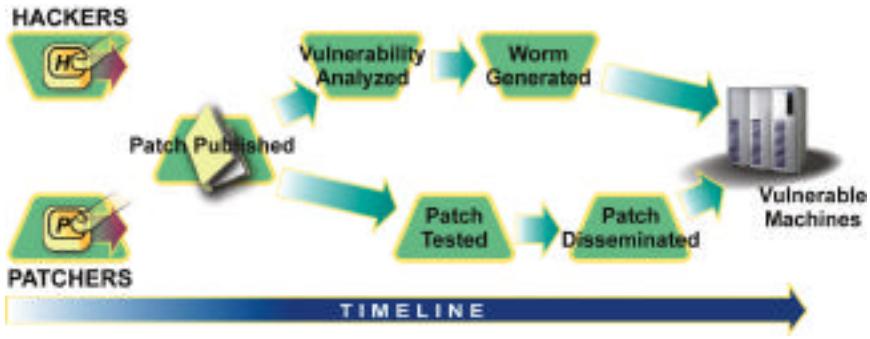

Figure 1. Hackers exploit the hole-patching process by developing worms for patches before they can be fully deployed.

The conference also explored notions related to "applications software," where security testing, auditing and traceability take a back seat to functionality testing related to performance specifications. In this scenario, there are elements in the software that are understood in terms of applications functionality or lack thereof, and there are elements in the software (particularly if it is legacy-based) that are not understood and thus create vulnerabilities and opportunities (see *Figure 2*).

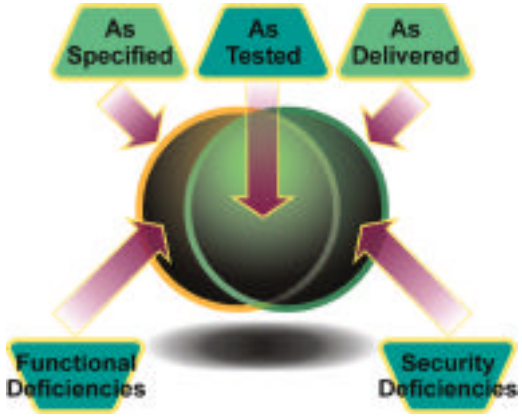

Figure 2. Information warfare is the science of probing the delivered system.

Finally, as one looks at generic concepts of applications that are surrounded by operating systems and subsequently surrounded by the graphical user interfaces (GUIs), application programming interfaces (APIs), files and kernels, one sees that many-faceted and varied ranges of attacks can be mounted on or from any of these layers (see *Figure 3*). The success of these attacks is enhanced when rigor in testing is lacking (this is particularly exacerbated when legacy vulnerabilities of poorly understood systems exist), or when software is not adequately tested because it is assumed to be "trusted."

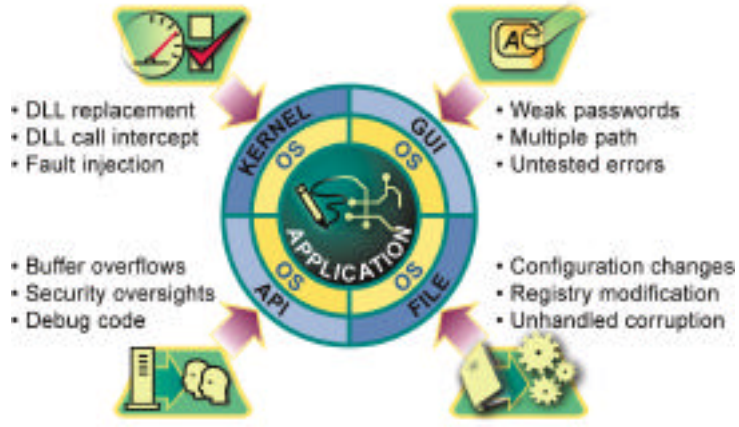

Figure 3. Applications surrounded by operating systems, and subsequently by the GUI, APIs, files and kernels, can be attacked on or from any of the many layers.

At the other end of the spectrum of threat and conflict is the evolving field of "information warfare" (IW), where the warfare capabilities are not proprietary to the United States, and the potential for mischief is not lost on U.S. adversaries. The objectives of an adversary's IW would be similar to our own. These would be premeditated and controlling, and they would attempt to influence our minds and our systems and capabilities, while seeking to maintain the superiority of their own abilities to "see, know, understand, decide and act," simultaneously depriving us of our abilities to do the same. The more a country or target depends on communications and IT (and the United States is utterly dependent in these areas), the more opportunities and vulnerabilities abound and risks increase.

Some ideas for the future

As we seek to win the game of assuring our systems and infrastructure, or at least dramatically improving our position, it is important to look for high-leverage strategies, processes and technologies in synergistic combination. The Army has long used the terms intelligence and operational "preparation of the battlespace." This term is being used increasingly in the joint military context, and it is being advanced in the context of cyber preparation. This involves *a priori* analysis and consideration of threats juxtaposed against leverage options for mission success, and it also involves laying the groundwork for achieving that leverage and success. There will be no perfect solutions or implementations, but rather, a layering of differentiated offensive and defensive means that, when synchronized around clever planning, supporting means and execution, are designed to prevail. The use of combinations of means, such as identification friend or foe (IFF), red (adversary) and blue (friendly) force tracking; credentialing of people; widespread encryption to secure communications or to authenticate activity; and offense-defense interaction, are all applied on the modern physical battlefield with leverage. However, their pervasive cyber-conflict direct analogs seem slower to evolve.

Strategies, engineering for enhanced deterrence and defense

As with modern battlefields, controls over actions of adversaries are problematic, and fixing the inherent weaknesses in one's own defenses is difficult, expensive and time-consuming. On the other hand, cost-effective strategies that deter adversaries, or that keep them out of the system, with the capability to point at agents of the adversary (or just malicious users) inside one's systems, could be useful. Adversaries are deterred only if they believe they will pay an unacceptable penalty for their actions. In the case of modern hackers, threats to their anonymity and misdirection of their attack actions pose potential threats; therefore, these threats become possible deterrents. This is also true of malicious insiders.

If each user (and perhaps hardware and software component) on a system is required to have some form of identity that cannot be repudiated, linked by certainty to that user's basic and known characteristics to enter and operate in a system, and if system operating enterprises granted their main privileges and functionality only on the basis of known participating identities, a powerful potential would exist for increasing integrity, security and trust in the system and its users. But even these solutions require extensive T&E.

Harnessing the power of identity

Public key infrastructure (PKI) can be employed to improve computer credentialing, define privileges and operationalize wider trust functions. Somewhere in the imaginative and perhaps unforeseen application of PKI, unexplored combinations of policy and technology options exist for greatly improving information assurance. Consider the power of some form of identity that cannot be repudiated. What if it were impossible to rob a bank without first submitting a notarized affidavit of identity, complete with bio-meds (current photograph, fingerprints, DNA, iris and so forth)? This would certainly reduce the number of bank robberies in the United States. Further, consider adding the power of privilege to some form of identity that cannot be repudiated. This would be akin to requiring the would-be robber, in addition to submitting a notarized affidavit of identity, to apply for a license from the bank to rob it. To obtain this license, the robber would have to meet a minimum level of background check to be issued a bank-robbing permit.

Imagine the modern battlefield full of adversary-recoverable IT systems needing protection when the protector is no longer functional. Can a bio-med-driven identity that cannot be repudiated help here? Imagine having sufficient trust in an IT system, that PKI functionality across the full spectrum of digital signature and encryption-related applications was managed differently and more effectively (in the background), because you know and trust all the users of the system. Sure, there are problems to be solved with regard to dealing with uncertified, unknown and poorly trusted or undocumented outsiders. Likewise, insider threats could still function, but the identity implementation would point directly and with certainty to attackers, greatly increasing their risks. Identity can pertain to people, things and data. Can we better employ concepts for identifying, tagging and authenticating software? Can further development around PKI enable us to fulfill the potential that PKI and digital signature concepts had promised over a decade ago?

The importance of T&E

As we look for high-leverage strategies, processes and concepts in the high-stakes game of information assurance, the T&E community—which lives with these evolving threats and vulnerabilities—can lead and evaluate. Testing must be optimized to take into account an understanding of the broader policies, processes, architecture, connectivity relationships (increasingly at the enterprise level), security strategies, forward and backward "use" and full-dimension "threat" contexts to prevent continued penetration and compromise of systems. It is in this broader context that the challenges lie for T&E. o

ADM William O. Studeman, USN (Ret.), is vice president/deputy general manager, Northrop Grumman Mission Systems, Reston, Virginia. ADM Studeman retired from the U.S. intelligence community after 34 years of service, where he served as Director of Naval Intelligence, Director of the National Security Agency and Deputy Director of Central Intelligence. He is a member of the Defense Science Board and other government advisory boards, and was recently appointed to the Presidential Commission on Weapons of Mass Destruction (WMD). ADM Studeman was assisted in this article by CAPT Bill Gravell, USN (Ret.); Ken Aull, Northrop Grumman Technical Fellow; and CDR Bob Gourley, USN (Ret), all of whom are experts in information assurance, including the use of advanced identity concepts and public key infrastructure (PKI) to enhance credentialing, as well as information technology (IT) and communications security.

Applying Science and Technology Research to Address Hyperspectral Sensor Test and Evaluation

The Department of Defense (DoD) is currently developing advanced multi- and hyperspectral sensors that span the electromagnetic spectrum from ultraviolet through millimeter wave. These emerging sensor systems represent a significant challenge to the test and evaluation (T&E) community. In Fiscal Year 2002, the Director, Operational Test and Evaluation (DOT&E), in conjunction with the Director, Defense Research and Engineering (DDR&E), established the Test and Evaluation/Science and Technology (T&E/S&T) Program to address S&T challenges affecting the T&E community's ability to test advanced weapon systems. One T&E/S&T focus area is addressing multi- and hyperspectral test.

A synthetic ground vehicle rendered using a Signature Research-developed tool, RenderView, and inserted into a measured scene

Current methods for testing multi- and hyperspectral sensors rely heavily on expensive field test programs. While these field tests provide realistic data for sensor testing, they leave several critical gaps. For example, test conditions are not repeatable. Environments observed one day will be different the next. Imagery can be collected and stored to partially mitigate this deficiency, but this process is expensive and cannot cover the full spectrum of environments required for complete test article evaluation. The T&E community needs the ability to test these advanced sensors in a repeatable, objective fashion before integrating them into warfighting systems. The T&E/S&T Program is addressing these needs through research efforts in scene generation, injection and projection to create test technologies that can be combined into integrated multi- and hyperspectral test capabilities.

One of the key technology developments underway is a next-generation signature model. The T&E/S&T Program is working with Aberdeen Test Center and Signature Research, Incorporated, to develop EOView, a multi- and hyperspectral signature model. EOView is able to merge multiple data sources, including thermal, atmospheric and radiation transport modeling techniques into a single hyperspectral data cube. EOView can estimate signatures at user-specified bands in the ultraviolet through infrared spectral region under a broad spectrum of operational conditions adaptable to the sensor under test. These scenes can be used to stimulate scene projection and direct injection systems or can define how sensors should perform in real-world situations to support T&E efforts.

EOView's physics-based thermal signature model incorporates high-fidelity targets with high-fidelity backgrounds. EOView provides advancement in modeling by leveraging both existing EO models and advanced high-performance computing hardware to create spectral radiometric scenes of unprecedented fidelity. Outputs will be hyperspectral data derived from the hundreds of millions of polygons that describe the target and terrain interactions using physics principles-based energy exchange. One feature of EOView is its ability to thermally integrate high-fidelity spatial targets and backgrounds, including dynamic target interaction with the terrain (plume, dust, smoke, tracks, shadows and so forth). The hyperspectral outputs of EOView can be tailored using the spectral response function of the sensor to create band images. The final version of EOView will be able to generate images across many spectral bands.

Once completed, EOView will be combined with other developments in the T&E/S&T Program to provide the T&E community with the ability to evaluate advanced multi- and hyperspectral sensor systems, under various environmental conditions, in a variety of geographical locations. This capability will be accomplished through generation of high-fidelity and phenomenologically correct images of targets and backgrounds that can be directly tailored to the sensor under test. ❑

This article was contributed by Dr. Mark Brown, T&E/S&T Program principal scientist; Marshall Weathersby and Dr. William Reynolds, Signature Research, Incorporated; and Frank Carlen, T&E/S&T Program multispectral test executing agent with Aberdeen Test Center.