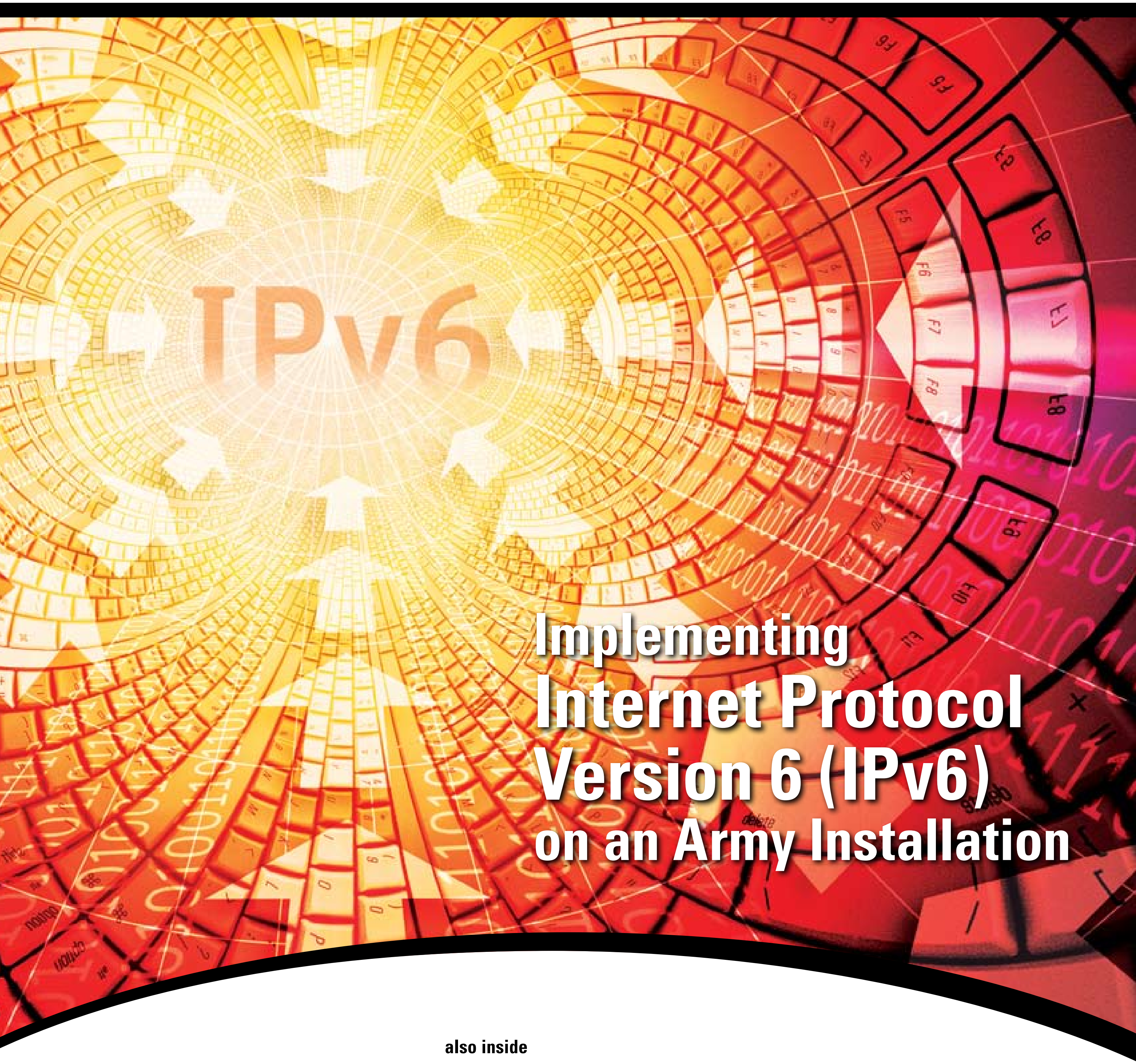
10/3

Volume 10 Number 3 • **Fall 2007**

IAnewsletter

The Newsletter for Information Assurance Technology Professionals



Implementing Internet Protocol Version 6 (IPv6) on an Army Installation

also inside

IATAC

contents

in every issue

About IATAC and the *IAnewsletter*
The *IAnewsletter* is published quarterly by the Information Assurance Technology Analysis Center (IATAC). IATAC is a Department of Defense (DoD) sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC), and Director, Defense Research and Engineering (DDR&E).

Contents of the *IAnewsletter* are not necessarily the official views of or endorsed by the US Government, DoD, DTIC, or DDR&E. The mention of commercial products and/or does not imply endorsement by DoD or DDR&E.

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

IATAC Director: Gene Tyler
Inquiry Services: Peggy O'Connor

***IAnewsletter* Staff**
Promotional Director: Christina P. McNemar
Creative Director: Ahnie Jenkins
Art Director: Don Rowe
Copy Editor: Louise Price
Designers: Bradley Whitford
Kacy Cummings
Michelle Deprenger
Editorial Board: Ronald Ritchey
Tara Shea
Gene Tyler
Buzz Walsh

***IAnewsletter* Article Submissions**
To submit your articles, notices, programs, or ideas for future issues, please visit http://iac.dtic.mil/iatac/IA_newsletter.html and download an "Article Instructions" packet.

***IAnewsletter* Address Changes/Additions/Deletions**
To change, add, or delete your mailing or email address (soft-copy receipt), please contact us at—

IATAC
Attn: Peggy O'Connor
13200 Woodland Park Road
Suite 6031
Herndon, VA 20171

Phone: 703/984-0775
Fax: 703/984-0773

email: iatac@dtic.mil
URL: http://iac.dtic.mil/iatac

Deadlines for future Issues
Spring 2008 January 4th, 2008

Cover design: Dustin Hurt
Newsletter design: Bryn Farrar
Donald Rowe

Distribution Statement A:
Approved for public release;
distribution is unlimited.

IATAC Chat

Gene Tyler, IATAC Director

I can hardly believe we are already nearly three-quarters of the way through the year. With so many great things happening in the Information Assurance Technology Analysis Center (IATAC), time has literally just passed me by. This year has been the year of publications for IATAC. With three publications already released and one on the way, we are thrilled with what we have accomplished and hope you are as well.

In our last edition, I discussed the two new State-of-the-Art Reports (SOAR) under development—the *Software Security Assurance* and the Insider Threat SOARs. The *Software Security Assurance SOAR,* released on 31 July 2007, has already been extremely well received throughout the information assurance (IA) community, including by our distinguished IATAC Steering Committee members. We are eagerly anticipating the release of the Insider Threat SOAR, which is well on its way to completion. However, I was a bit overzealous with its mid-September target release date—stay tuned for release updates.

In addition to the new SOARs, we published two new Tools Reports. The purpose of each of our Tools Reports is to give the reader a bit of background on the tool (what it is, what it does, what it doesn't do, *etc.*) and an index of various types of tools available in each of the three categories: Firewalls, Intrusion Detection (IDS), and Vulnerability Analysis (VA). On 14 May 2007, we published updated versions of both the IDS and VA reports. The IDS report provides a summary of the characteristics and capabilities of publicly available IDS and Intrusion Prevention Systems (IPS). The VA report provides information on risk assessment and risk management concepts. Although IATAC has researched and written the background and information primer portions of these reports, we do not endorse, recommend, or evaluate the effectiveness of any specific tool. The descriptions of the tools are based solely on vendors provided information and are intended only to highlight the capabilities of each tool. If you are interested in any of our new or past publications, please visit our website, *http://iac.dtic.mil/iatac*, or email us at iatac@dtic.mil.

In this edition of the *IAnewsletter,* you will once again find several focused and indepth articles, including Information Assurance for the "Net-Centric Environment: Making the Mission Possible." This is a fascinating article that looks at two unique questions. First, how do we best protect the Global Information Grid (GIG) from our adversaries and secure it for use in a variable-trust environment? Second, how must our IA strategies differ from those we have used in the past? Also, this edition includes a captivating article related to computer network defense and NetOps. "Executing the CND Data Strategy Within the NetOps Community of Interest" takes a look at the development and implementation of a Net-Centric data strategy. As always, you will find several other intriguing articles as well as our recurring features. ■

Gene Tyler

Implementing Internet Protocol Version 6 (IPv6) on an Army Installation

by Trace Gunsch

Abstract

With Department of Defense (DoD) and Office of Management and Budget (OMB) mandating a migration to IPv6, Army installation Directors of Information Management (DOIMs) are beginning to feel pressured to implement IPv6 on their post networks. Unfortunately, little practical guidance exists to inform the DOIMs the procedures necessary to prepare their networks for IPv6. More is needed than simply enabling IPv6 on local area network (LAN) routers and switches. Many infrastructure components must be upgraded as well, including Domain Name Service (DNS), directory services, security, and network management. Besides the physical hardware and software components, local policies need to be defined for network security and IPv6 addressing, and steps need to be taken to provide training for administrators and registration of IPv6 pilots.

This article summarizes the steps necessary to enable an IPv6 pilot on an Army post. It attempts to address the question, "What is necessary to do today to prepare for an IPv6 application on the post network tomorrow." It covers the procedures necessary to implement IPv6 on an Army base, including covering current status of commercial product support and Government testing of IPv6 capabilities.

When DoD first began implementing communications networks using Transmission Control Protocol/Internet Protocol (TCP/IP), network protocols were fairly immature. Configuration of devices was manual, security and prioritization were absent, network management was immature, and communications speeds were incredibly slow by today's standards. Over time, our IP networks have become more robust, more user-friendly, and equivalently more relied upon by users and managers. Our users now expect a high level of performance from our IPv4 networks. We have in-depth security systems, highly robust network management, auto-configuration, prioritization, converged voice and video, multicast, mobility, and high-speed performance capabilities on our IPv4 networks.

The challenge of implementing IPv6 into an Army network comes from two conditions placed upon the DoD by the US Congress: Do No Harm and IPv4 Parity. The first is easily understood and met—we do not want to diminish our current communications capability in order to develop a future capability. The second is the real challenge—that the IPv6 network will perform equivalent to or better than the current IPv4 network.

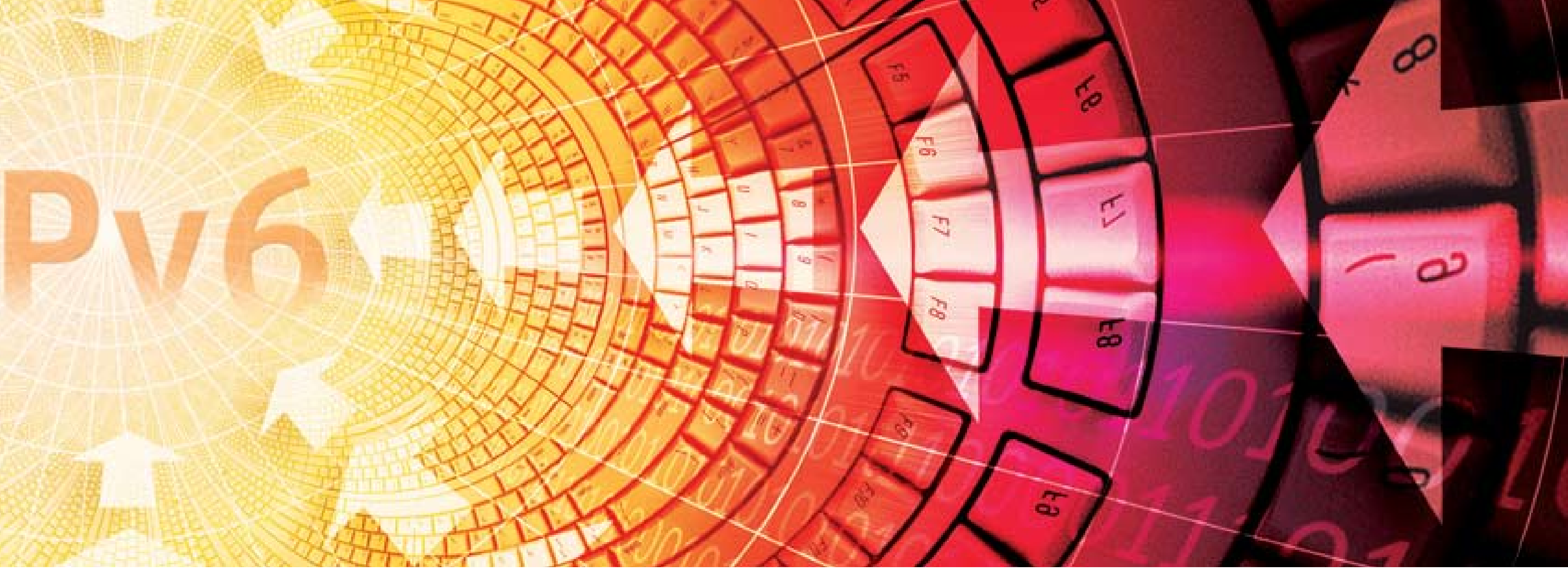
The upside of IPv6 implementation is that most IPv4 vendors are now moving to support IPv6 in the same devices that currently run our IPv4 networks. The downside of IPv6 implementation is that the equivalent features and capabilities of IPv6 tend to lag several years behind IPv4.

This paper investigates the network service areas of a typical Army post and shows what can be achieved now with IPv6 and what lags behind in achieving IPv4 parity. It describes the current state of industry and the pieces which need to become mature before we can implement IPv6 on our networks with IPv4 parity.

Background

In June 2003, DoD Chief Information Officer (CIO) published a memorandum requiring a migration of DoD networks to IPv6. [1] This memo, and a September 30 follow-on, defined that the IPv6 transition would be accomplished through technical refresh cycles, and that all future purchases should be of IPv6-capable products, with a loose definition of what IPv6-capable means. [2] The hope was that by 2008, all network devices would be IPv6-capable and enabling IPv6 would be relatively simple and cost-effective.

The fallacy of this approach is that the products available for purchase in 2003 were not really IPv6-capable, and continuing progress has not generated IPv6-capable products. It was well known in 2003, that several Asian countries were building IPv6 networks, but the commercial products available at that time did not have the capabilities of IPv4. For example, Gigabit Ethernet (GbE) switches, which pass IPv4 packets at rates of 1 billion bits per second could only pass IPv6 packets at less then 1 percent of that rate. This may not have been an issue for China, which had little to no IPv4 infrastructure—to them, any IPv6 capability is an



improvement—but it stymied DoD deployments. Even now, four years later, many capabilities regularly found in IPv4 products are not available in IPv6 implementations, and vendors are more motivated to build new IPv4 capabilities than to improve IPv6.

IPv6 Pilots

As stated previously, one of the DoD goals is transition through technical refresh. Communications hardware often gets replaced every three to five years. Replacing the hardware with IPv6-capable products, if they existed, could be accomplished with little additional cost. The technical refresh approach, however, does not solve all the needs of a transition to IPv6. At best, it can cover much of the hardware and software cost of the migration; but it fails to address many other issues such as testing, modeling and simulation; developing policies; changing security architecture; increased operations and maintenance; and training.

The DoD's solution to these gaps in the implementation is through the extensive use of pilot programs. A pilot is considered to be an intermediate step between test and implementation. The DoD hopes to eliminate much of the costs of testing and training through the use of service pilots and has been pressuring the services to identify pilot candidate programs and to begin testing IPv6 in constrained implementations.

DoD Milestone objectives

In addition to the two DoD memoranda mentioned previously, numerous different mandates and memos from DoD, OMB, and Assistant Secretary of Defense for Networks and Information Integration [ASD(NII)] provide guidance for implementing IPv6 on Government and DoD networks. A listing and short description of all these documents are listed at the end of this article. References 9 and 10 established the following milestone objectives for conducting an IPv6 pilot.

a. **Milestone Objective 1 (MO1)** states that services and agencies are authorized to operate IPv6 systems within an enclave. The MO1 allows the use, familiarization, and testing of IPv6 protocol and applications for operational pilots in order to ascertain issues and derive migration strategies. Pilots are authorized to operate at MO1, effective 1 October 2005.

b. **Milestone Objective 2 (MO2)** provides the ability to evaluate the scalability and further evaluate the IPv6 Information Assurance (IA) implications using tunneling and native IPv6 routing, as available. The MO2 permits applications to test IPv6 specific end-to-end capabilities and routing schema efficiencies. Pilots are authorized to operate at MO2, effective 1 December 2006.

c. **Milestone Objective 3 (MO3)** will be authorized when all policy, planning, and technical transition guidance has been provided to allow tunneled and native IPv6 traffic to exist on DoD operational networks. The MO3 will permit applications and data owners to complete operational transition to IPv6 with at least the same functionality as currently found in IPv4. Target date for MO3 is Fiscal Year 2008.

Enabling IPv6 for an Army Pilot

The Army is considering leveraging the Installation Information Infrastructure Modernization Program (I3MP) to conduct a pilot for IPv6 on an installation. The Army's I3MP provides for the engineering, acquisition, implementation, and management of the Army's installation level telecommunications infrastructure. While I3MP is primarily responsible for Ethernet switches which compose the network backbone, a pilot cannot simply be enabling IPv6 on a couple of switches or routers. An effective pilot requires an IPv6 application running across the post infrastructure, demonstrating the operation of IPv6 end-to-end.

At the I3MP program manager's request, engineers at USAISEC conducted an analysis to determine how to enable an IPv6 pilot on an Army post. Our approach to this analysis was to answer the question, "What do we need to do on the post today to be ready for IPv6 application tomorrow?" We scoped the problem with a couple of assumptions:

a. Every affected device in the system will be dual-stack, supporting IPv4 and IPv6. This includes the application server, client, and network backbone. There will not be any IPv6-only devices and no tunneling.

b. The application will reside entirely on-post. The client and server machines will all be on the same post and no IPv6 traffic will leave the post. This meets the MO1 guidance.

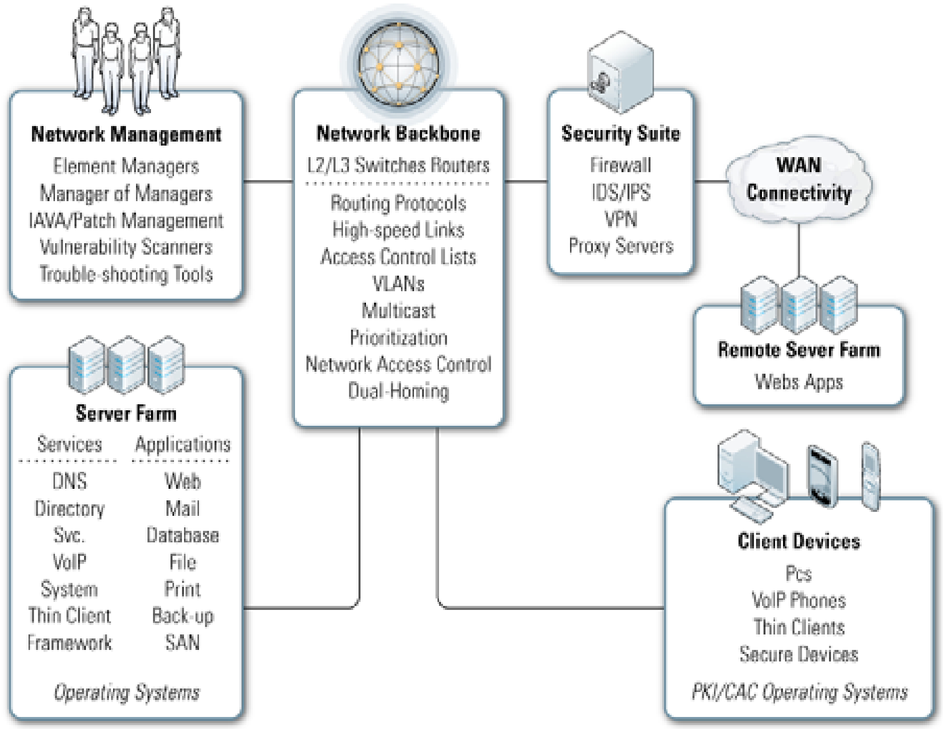


Figure 1 I3MP Architecture – System View

Requirements

Figure 1 shows the typical architecture of an Army installation network or any campus network. The network backbone typically consists of IP routers and switches overlaid on some type of Layer 1 (L1) and Layer 2 (L2) communications technology (Asynchronous Transfer Mode, Ethernet). This backbone provides connectivity for the central server farm, network management stations, and client devices. The Army post connection to the Internet is protected by a security suite, through which all external traffic must traverse.

Post-wide Requirements

Several issues must be addressed that will affect all aspects of the IPv6 implementation. These are policy, addressing, and training. For policy, current DoD directives state that IPv6 traffic is not allowed on any operational DoD Network, except under a pilot project. The DoD IPv6 Transition Office (DITO) has established that any DoD pilot must adhere to the MO1 and MO2 guidance and must be registered with the DITO. Another policy issue relates to security. A pilot implementation must define appropriate security policies of what IPv6 traffic will be allowed on the network and where that traffic will be allowed to go. This will be discussed more in the section on the Security Suite.

An address plan is necessary before establishing IPv6 traffic. Most IPv6 experts suggest that a post IPv6 address plan should closely reflect the current IPv4 addressing plan, to ease network management, but opportunity exists to improve the addressing scheme in IPv6. Addresses should be given out in a manner that will facilitate hierarchical routing, where prudent, and should follow Army and DoD addressing policies. Unfortunately, Army and DoD addressing policies are not complete at this time, and so a post cannot at present obtain permanent IPv6 address space.

The final global requirement is equipping the network administration team, who will be responsible for troubleshooting network problems and enabling IPv6 on the network. Network administrators require training on the IPv6 protocols and require tools that can analyze both IPv4 and IPv6 traffic. The availability of such tools is discussed in Zone 6.

Network Backbone

The backbone of an Army network typically consists of a handful of Layer 3 (L3) Ethernet switches which support connections to the user buildings. The user buildings are connected Ethernet switches or other L2 technology. The L2 devices do not deal with traffic at the IP layer, so do not have to support IPv4 or IPv6, other than to support remote network management access (see the following).

Current I3MP requirements dictate that L3 switches must meet full performance parity of IPv6 and IPv4. [3] This means that those switches must be able to transmit the full 1 or 10 Gigabits per second on each GbE or 10-GbE port. In addition, they must have support for Open Shortest Path First (OSPF) version 3 (the IPv6 equivalent of OSPF version 2), and must support IPv6 Access Control Lists (ACLs) and security logging. Often an L3 switch will be dual-homed, so if one link fails, the other will automatically take over. This should be a requirement for IPv6 traffic as well as IPv4. Lastly, all IPv6 devices must support Internet Protocol Security (IPSec), according to IPv6 standards and the DoD Information Technology Standards Registry (DISR) Product Profile. [4]

Of these requirements, several L3 switches exist which meet the performance, OSPFv3, and ACL/security logging requirements; but none tested at the TIC have met the IPSec requirements to date. We have not tested dual-homing capabilities for IPv6 to date, so that capability is unknown. Additional I3MP requirements go into effect on 1 Jan 2008, [5, 6] requiring L3 switches to fully support IPv6 network management and IPv6 security, equivalent to current IPv4 standards.

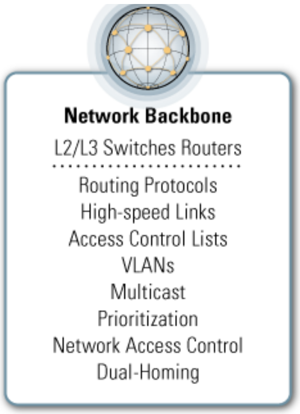


Figure 2 Network Backbone

Several other features of network backbone devices are considered optional or "nice to have." These features are necessary for full IPv4 Parity, but an IPv6 pilot can operate without them. These optional features include Differentiated Services (DiffServ) for traffic prioritization, tunneling IPv6 over IPv4, multicast, virtual LAN (VLAN), 802.1X, and auto-configuration support. Of these features, DiffServ, auto-configuration, and tunneling are common to commercial Ethernet switches, but secure network management, multicast, and 802.1X support are not. Support for IPv6 VLANs is widely varying among current switch vendors.

The DoD recently reduced the IPSec requirement for switches and routers. These devices must pass IPSec traffic without modification, but secure network management over IPSec is not required at this time. IPSec support, for now, falls in the "nice to have" category.

Client Devices

A typical IPv6 application will communicate between a client and a server across the network. For the assumed scenario, some number of client computers will need to be IPv6-enabled. This will require a computer operating system (OS) that can run in dual-stack mode. Most commercial OSs can do this; LINUX, Solaris, Macintosh, and Windows Vista all support IPv6 fairly well. Windows XP lacks many IPv6 capabilities, so it should not be used for a pilot.

In addition to a dual-stack OS, the client system needs some sort of auto-configuration support from the network. Dynamic Host Configuration Protocol (DHCP) is not mature in IPv6, so switch-based auto-configuration is the preferred method, and it is supported in most L3 switches.

Those are the minimum requirements; however, several features that users expect from their client devices are not mature for IPv6. Public Key Infrastructure (PKI) and common access card (CAC) support, for example, are not developed yet for IPv6. Active Directory and thin client support for Microsoft OSs are not established yet for IPv6, either, though Microsoft promises these features in their next server OS, Longhorn, due in late 2007. Dynamic Domain Name Service (DDNS) is also not mature for IPv6. The DDNS is highly valuable for network managers, who otherwise have to manually enter every IP address into static DNS tables. Manual entry is very time-consuming and error-prone with IPv4; much more so with IPv6. This also is promised in Longhorn. Support for DDNS in other OSs is unknown.

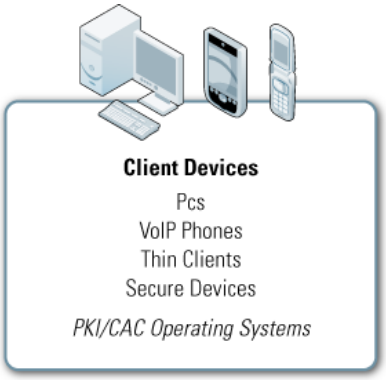


Figure 3 Client Devices

Finally, the issue of user applications is critical to IPv6 deployment. At present, few commercial applications exist that fully support IPv6, and it is incredibly rare to find one that uses features of IPv6 that IPv4 cannot support. This is a major issue in the push for IPv6 deployment: without applications that use IPv6 features, the motivation to migrate to IPv6 is very low, and the momentum to improve IPv6 capabilities in network devices is very small.

Server Farm

The server farm is where the domain controllers, mail, file, and other application servers reside. It is typically a centralized location where the network administrators can conveniently maintain hardware components, monitor security patches, and conduct system backups. For an IPv6 implementation, the required components are an IPv6-capable DNS system and a dual-stack OS on the server that will host the IPv6 application. Other server farm components, such as DDNS, Active Directory, and back-up tools, are optional to run on IPv6 at this time.

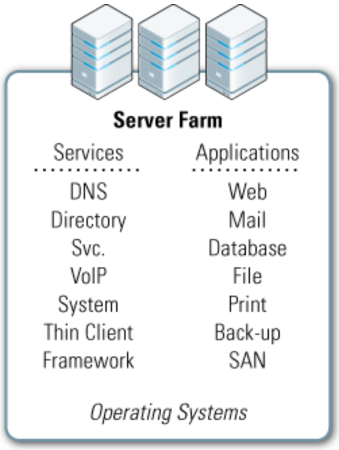


Figure 4 Server Farm

Commercial DNS products have supported IPv6 for several years; in fact, DNS is one of the first aspects to fully support IPv6. Dual-stack OSs are coming along. Most UNIX platforms support most IPv6 features, but Windows 2003 does not. Microsoft's Longhorn, due out in late 2007, promises built-in IPv6 support, including Active Directory and DDNS support over IPv6. Longhorn will require a 64-bit server bus, which means many DOIMs will have to upgrade their server hardware to implement it. Once released, users should expect several months before Network Enterprise Technology Command (NETCOM) policy allows Longhorn's implementation on Army networks.

Standard office applications do not typically make use of IPv6 features and often do not support it. Microsoft's Exchange 2007, for example, just released this year, will not support IPv6 until

Service Pack 1, due out in late 2007. Other applications are at various stages of IPv6 implementation. Many UNIX-based thin client systems support IPv6, but Microsoft's thin client support for IPv6 is unknown. Voice over IP products presently do not support IPv6, so providing an IPv6 call processor system will be very difficult. Even more challenging will be the thousands of Army-specific applications that will need to be upgraded to IPv6 support at some time. Most of these applications do not require IPv6 support for a pilot project, but these are issues Army users need to start considering.

Network Management

Network management over IPv6 will often be one of the last areas enabled for an IPv6 implementation. Devices that use IPv6 traffic in a dual-stack mode can be managed using IPv4, without any impact to the IPv6 traffic. Network management is also the least mature of the IPv6 technologies in the commercial realm. It will eventually become a requirement when the Army moves to IPv6-only deployments, and with that goal in mind, I3MP is requiring IPv6 network management in L3 switches starting in January 2008, but few vendors presently show much capability in this area.

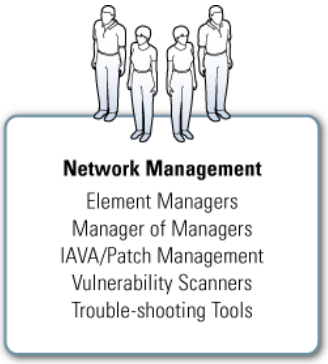


Figure 5 Network Management

Element manager tools, such as Hewlett-Packard OpenView and Spectrum, use secure Simple Network Management Protocol (SNMP) over IPv4 to manage network devices, but presently do not support secure SNMP over IPv6. Patch management tools, such as Systems Management Server (SMS) and anti-virus updates currently cannot be accomplished over IPv6. Again, these tools do not need to run over IPv6 for a network to support IPv6, but we will eventually need this capability when we leave our dual-stack environments for IPv6-native deployments.

Network management includes the ability to scan networks for hostile IPv6 traffic, IPv6 viruses, and vulnerabilities to IPv6 attacks. It also includes the ability to analyze traffic patterns and tools for troubleshooting and optimizing networks. These tools are things DOIMs use frequently in their day-to-day operations and are vital for deploying and maintaining an operational or a pilot network. Some network sniffers, such as Ethereal, support IPv6, but the status of vendor development for other scanning tools varies, and DOIMs will need to determine if the tools they presently use can support IPv6.

Security Suite

For any campus network, the security suite protects the network from external intrusions and attacks. For the Army, it is typically installed and managed by NETCOM, instead of the local DOIM. Figure 5 shows the typical components, from NIPRNet connection to the network core. It also shows a remote server farm, where a global application might be hosted.

Our initial conditions for this paper stated that an IPv6 application would not leave the local post. This means that the security suite really is not involved in passing IPv6 traffic. The only thing necessary in the TLA stack is to block IPv6 traffic from crossing either direction. Current firewalls do this by default, so no action is necessary at the security suite for a local pilot implementation.

However, the Army is moving toward regional server consolidation, so remote applications are desirable. If an IPv6 application were to be hosted at a remote location, several new requirements emerge. First of all, some sort of tunneling mechanism will be required between the remote server and either the local servers or the client machines. The tunnel mechanism must encapsulate the IPv6 data into IPv4 packets to ship across the NIPRNet. Tunnel mechanisms exist, but they create a new requirement for security devices, firewalls, and intrusion detection systems (IDSs). In a tunnel, IPv6 packets are encapsulated within IPv4 and usually encrypted. This makes deep packet inspection, required by current Defense-in-Depth policies, extremely difficult. Security as an industry is far behind in the deployment of IPv6, and finding IPv6-inspecting firewalls and IDSs is challenging.

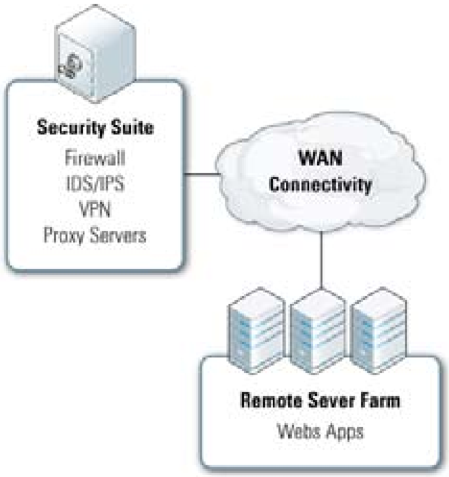


Figure 6 Security Suite

An alternative solution to tunneling is to use IPv6-capable virtual private networks (VPNs) to encrypt IPv6 traffic between the local post and the remote servers. This removes the requirement for a tunneling device and bypasses the issue of packet inspection on firewalls and IDSs because encrypted traffic cannot be inspected. This approach is counter to the current security policies, however, and much collaboration is needed between DoD and Army security architects and IPv6 implementers to work through these security issues.

Eventually, we will need to open up the entire network to IPv6 traffic, so that IPv6 applications can communicate between any military posts and to the Internet. When that time comes, we will need full IPv6 support on firewalls, IDSs, VPNs, and proxy servers. Current security routers may require hardware upgrades to support dual-stack, and industry will have to start building IPv6 capability into these security devices, which at present have very little IPv6 support.

When Will We Get There?

A lot of the delays to DoD's IPv6 implementation occur because commercial vendors do not see the pressing need to migrate to IPv6. Twenty years ago, DoD was a dominant customer in the communications industry and DoD directives were taken very seriously by industry. Today, DoD represents a relatively small market segment for most commercial vendors. To make matters worse, DoD as a whole is not investing money into IPv6 development and is only half-heartedly promoting IPv6 implementation on its networks. It is a classic catch-22; DoD agencies do not want to invest a lot of money into IPv6 until industry starts making better products, but industry does not want to spend a lot of money developing IPv6 products until customers start buying them.

Some glimmers of hope do exist, though. The DoD has established a number of testbeds where IPv6 capabilities are being evaluated and products are being recommended for implementations. For example, the Army's TIC has established an IPv6 System Integration Facility for validating IPv6 capabilities for hardware, software, and systems. Under the sponsorship of I3MP, this lab is testing Ethernet switches, routers, OSs, and security devices. They also are testing commercial applications and are able to test Army-specific applications in a replicated Army post environment.

The DoD has also established an Approved Products List (APL) of commercial products that have demonstrated conformance to DoD standards, interoperability with DoD equipment, and a certain level of performance in IPv6. As the APL gets populated, the DoD intends to mandate that only products on the APL can be purchased and used on DoD networks.

Issues/Concerns

Several concerns are prevalent in any implementation of IPv6; Internet Protocol Security (IPSec) is one of the most controversial. Current guidance states that all IPv6 devices must support IPSec. Current National Security Agency (NSA) Guidance appears to indicate any IPSec device is an IA device and therefore must undergo Federal Information Processing Standard (FIPS) certification and National Information Assurance Partnership (NIAP) Common Criteria evaluation. The majority of IPv6 devices available at present do not support IPSec. Both the development of IPSec capabilities and the FIPS/NIAP processes are very expensive for vendors and time-consuming, meaning extensive delays in getting secure products for DoD implementations. With DoD's recently reduction of this IPSec requirement for switches and routers, this concern is reduced somewhat for the network backbone, but it is still a concern for IPv6 deployment.

Another issue, touched on in the server farm discussion, is that upgrades are required for most servers to support the 64-bit bus speed required for Longhorn. The NETCOM has proactively mandated that future server purchases must be 64-bit, but the bulk of current servers are only 32-bit.

Finally, the issue of addressing policies is not yet defined for DoD and Army. A pilot implementation could proceed with temporary IPv6 addresses, but unless an addressing plan is defined, implementers risk wasting a great deal of time and effort in renumbering and restructuring a pilot implementation when the addressing plans are finalized.

Conclusions and Recommendations

Implementing IPv6 on an Army Post requires many more components than just IPv6-enabling core elements. Besides the switches, implementers need to be concerned with server and client OSs, network scanning and vulnerability analysis tools, addressing plans, policies, and training. Commercial products for these aspects are lacking in IPv6 development, so conducting pilots at this time is very difficult.

The DoD needs to continue to encourage industry to develop IPv6 products. The DITO should publish a mandate now requiring APL usage at some future date and encouraging vendors to submit their products for APL testing. Army program managers need to pressure vendors to develop IPv6 capabilities now in their products and applications and pursue testing, at facilities such as the TIC, to confirm that they will work in the Army secure dual-stack environment. ■

References

1. DoD CIO Memorandum, Internet Protocol Version 6 (IPv6), 9 June 2003.
2. DoD Chief Information Officer (CIO) Memorandum, Internet Protocol version 6 (IPv6) Interim Transition Guidance, September 29, 2003.
3. Program Executive Office, Enterprise Information Systems (PEO EIS) Memorandum, Approved Product Performance Specification for Internet Protocol Version 6 (IPv6), 7 June 2006.
4. DoD CIO, Department of Defense Information Technology Standards Registry Baseline Release 05-2.0 (DISR), September 6, 2005.
5. PEO EIS Memorandum, Recommended Product Management Specification for Internet Protocol Version 6 (IPv6), October 2006.
6. PEO EIS Memorandum, Recommended Product Security Specification for Internet Protocol Version 6 (IPv6), October 2006.
7. DoD CIO Memorandum, Internet Protocol Version 6 (IPv6) Transition Plan Coordination and Interim Tasking, 28 November 2003.
8. OMB Memorandum, M-05-22, Transition Planning for Internet Protocol Version 6 (IPv6), 5 August 2005.
9. DoD CIO Memorandum, Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Master Test Plan, 16 August 2005.
10. DoD CIO Memorandum, DoD Internet Protocol Version 6 (IPv6) Pilot Nominations, 16 August 2005.
11. DoD CIO Memorandum, Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Implementation Schedules for Major Networks and Programs, 18 July 2006.
12. Assistant Secretary of Defense, Networks and Information Integration [ASD(NII)] Memorandum, Internet Protocol Version 6 (IPv6) Policy Update, 16 August 2005.

List of Mandates

a. DoD CIO Memorandum, Internet Protocol Version 6 (IPv6) (also known as the Stenbit Memo), 9 June 2003.
   - Directed that as 1 October 2003, all Global Information Grid assets being developed, procured, or acquired shall be IPv6 capable (in addition to maintaining interoperability with IPv4 systems/capabilities).

b. DoD CIO Memorandum – 29 September 2003, Internet Protocol version 6 (IPv6) Interim Transition Guidance
   - Established policy that products and systems procured or acquired after 1 October 2003 must be capable of operating in IPv6 networks.
   - Defined IPv6-Capable.
   - Identified the Joint Technical Architecture IPv4/IPv6 IT standards Profile as a reference.
   - Established provisional process and requirement for Component CIO waiver when IPv6-capable criteria cannot be met.

c. DoD CIO Memorandum – 28 November 2003
   - Required DoD Components to develop *Transition Plans* no later than April 2004, and include resource requirements in program objective memorandum and budget submissions.
   - Required NSA to develop security guidelines and solutions, and take actions to ensure availability of IA-certified products to support fielding.
   - Required NSA to develop IA and Network Connection Guidelines for IPv6 Pilots.

d. OMB Memorandum – 5 August 2005
   - Set June 2008 by which all agencies' infrastructure (*network backbones*) must be using IPv6.

e. ASD(NII) Memorandum – 16 August 2005
   - Defined *Milestone Objectives* for enterprise-wide deployment of IPv6.
   - Established Components' authority to determine their waiver policy.

f. DoD CIO Memorandum – 16 August 2005
   - Established DoD Chief Information Officer-Executive Board (CIO-EB) and *Information Technology Standards Guidance (ITSG)* for oversight of planning.
   - Required Components to nominate O-6/GS-15 ITSG representatives.

g. DoD CIO Memorandum – 16 August 2005
   - Established requirements for nomination, planning, and implementation of *pilots*.
   - Requested Components to nominate pilots.
   - Authorized pilots to commence on 1 October 2005, subject to meeting required conditions.

h. DoD CIO Memorandum – 18 July 2006
   - Required Components to submit *IPv6 Implementation Schedules* for major networks and programs.
   - Requires Components to submit quarterly updates to DoD CIO-EB on transition progress.

About the Author

Mr. Trace Gunsch | is the Emerging Technologies CSE at the USAISEC-TIC, Fort Huachuca, Arizona. He holds a Bachelor of Science Degree in Engineering Physics from North Dakota State University and a Master of Science Degree in Electrical and Computer Engineering from the University of Arizona.

ASK THE EXPERT

Paradigm Shift

by Jack Phillips

Talk about a divide between the old and the new! We recently celebrated the Institute's 6-year anniversary, with 150 security professionals from the financial services sector in New York City. Gone are the days of significant attention being paid to sealing or defending the perimeter:

The new paradigm of encrypting data at rest and in motion, along with limiting access to data through key infrastructures or digital rights management (DRM) systems, has taken hold of the commercial sector.

What is remarkable is how different the problem set now is when protecting data rather than defending certain architectural zones. The primary challenge today is effectively quantifying the value of data assets and then limiting access by user profile. Combining these two disciplines is

"The odds are now so stacked against having success at the perimeter level. The big bad world outside our walls is just moving too fast. Now everything we do is at the data level. Encrypt anything and everything is our new mantra…figure out if it's valuable later."

leading to significant complexity, which in turn is damaging productivity.

The three areas described below (*i.e.,* database encryption, mobile/wireless encryption, laptop and file/folder level encryption) are seen as garnering the most attention today.

Database Encryption

In a simplified way, security professionals historically perceived databases as situated so deep within networks that multiple perimeter defenses would surely protect any unauthorized access to them. Numerous factors have negated this belief, and nearly every commercial security team now has a "data at rest" security program in place.

Database encryption is a difficult problem primarily because of the key management issue. Many commercial solutions available tend to provide a false sense of security if not implemented correctly. Simply deploying database encryption before thoroughly understanding how the key is protected will not provide the expected security.

The fundamental problem concerns how data in the database can be made easily available, yet allow easy access to the key without manual intervention. If the key is so easily accessible that data could be decrypted on the fly, then an attacker could easily decrypt the information, negating any benefit gained through encryption. The best solution is to integrate key management into the database application.

Mobile/Wireless Encryption

With an explosion of mobile access in the commercial sector, wireless and mobile encryption has become a hot area. The difficulty is that the product area is evolving. No single solution can handle all existing operating systems (OS) and form factors (*e.g.,* Windows, UNIX, Linux, Mac, Palm, RIM BlackBerry). Most products support Windows, and one or two mobile device OSs. Only a few support Linux, and virtually none support Mac OS 10.

The most successful security teams and business owners work upfront to identify mobile devices with critical data

(*i.e.,* those in the hands of senior managers and C-Level executives, as well as mobile employees with high-value business data). This effort will allow for limitations in the scope of an encryption deployment, making it easier to manage.

Laptop and File/Folder Level Encryption

Most organizations we follow began their data protection process by first identifying business requirements and then considering whether full-disk (*e.g.,* laptop or device being stolen) versus file/folder level encryption (*e.g.,* information leakage protection) is the most appropriate approach.

The strongest use case for full-disk encryption products is for laptops or portable hardware that is lost or stolen while powered off or not logged in. As long as the password protection and authentication policy in place is strong, data will be protected. A benefit of full-disk encryption is that it is more seamless to the user and not necessarily subject to "pilot error," as is partial data encryption. However, if not rolled out with an enterprise edition and master key, part of the OS where patch management tools need access to keep the machine up-to-date will be encrypted without an ability to decrypt without the user, leaving the machine vulnerable.

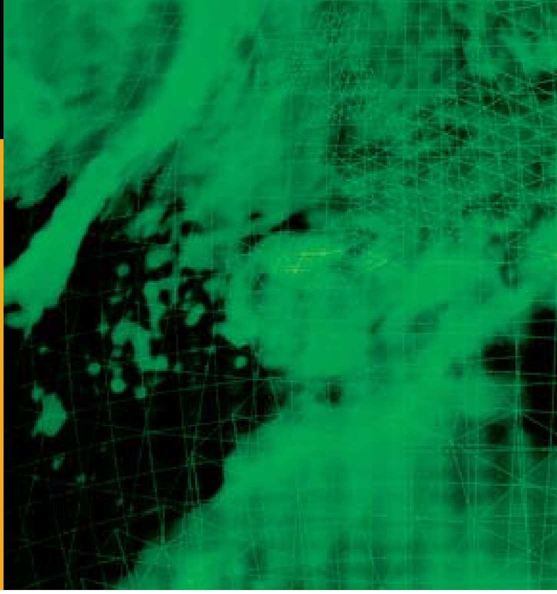
A benefit of partial data encryption is that if an encrypted file/folder is moved or sent elsewhere, then it remains encrypted. Each encrypted file/folder has its own password, whereas full-disk encryption is only as strong as the password and authentication policy in place. A deficiency of partial data encryption is that Microsoft Windows puts cache files, temp files, and paging files in different locations. Those files might contain sensitive data and would be placed outside an encrypted folder.

Taken together, data encryption techniques coupled with access protocols are in their infancy. The zeal to encrypt as much as possible is creating significant productivity challenges for many commercial organizations. However, like so many other mature security technologies, going forward, data encryption will be the cornerstone of digital commerce and communication. ■

About the Author

Jack Phillips | began his career in media and information publishing as an investment banker at Morgan Stanley & Co. in New York. After filling senior operating positions at McGraw Hill beginning in 1994, Mr. Phillips joined the founding team of Internet Securities in 1995 (subsequently purchased by Euromoney in 1998) and later joined CCBN.com in 1999. Mr. Phillips left CCBN.com in mid 2000 to launch the IANS. He is a graduate of Williams College and the Harvard Business School. He may be reached at the Institute for Applied Network Security, 15 Court Square, Suite 110, Boston, MA 02108, by telephone at 617 399 8100, or by email at jphillips@ianetsec.com

A Qualia Framework for Awareness in Cyberspace



by Timothy H. Lacey, Robert F. Mills, Richard A. Raines, Paul D. Williams, and Steven K. Rogers

Abstract

As the newest mission area for the US Air Force, cyberspace is getting a lot of attention, and rightfully so. Every person, system, and device that communicates via the use of electronics and the electromagnetic spectrum is a part of this fascinating domain. Cyberspace is not new…it has been around for many years. However, our understanding of how this domain can be exploited has increased dramatically in recent years. As users and managers of cyberspace, we need to know what is happening in this domain. More importantly, we must know how to defend our cyber resources, exploit an adversary's use of the domain, and hold the adversary's operations at risk if need be. All of this requires cyberspace awareness. This is not your grandfather's awareness (one-size-fits-all data overload), but awareness based upon what is relevant to each individual at any level of the command hierarchy, presented in a useable form. The objective is to attain universal situational awareness, defined as awareness across all media and including all the hierarchy.

Military operations are increasingly dependent upon information technology and communication networks. Cyberspace, as defined by the Department of Defense (DoD), is "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data *via* networked systems and associated physical infrastructure." [1] Cyberspace is a supporting domain that enables operations in air, land, sea, and space. It is also an operational domain in which targets are attacked and defended, and effects are realized to achieve some overall military or political objective. Recognizing this, the US Air Force has changed its mission statement to include cyberspace as a mission area and has begun organizing, training, and equipping a cyberspace force. [2]

A very significant problem is linking physical domain activities and processes to cyberspace. Network support personnel have long found it difficult to determine the impact that a network failure or disruption will have upon the mission(s) being supported. It is difficult to analyze the specific impact the event has on the mission because the links to the users' particular missions or business processes are not readily known. [3]

The problem stems from the fact that network support personnel and end-users speak in different languages. For example, Air Force commanders speak in terms of "time-over-target," "engagement areas," and "effects based operations." Network administrators, on the other hand, tend to focus on the network, and use terms such as "bits per second," "bandwidth and throughput," and "network latency"—these terms mean nothing to the commander who just wants to know "so what?" when briefed about a network failure or incident.

The commander and network administrators represent two extremes—there are many other people in between who also have either some dependency upon or role in maintaining the network infrastructure. Depending on each person's function, their desired "map" of cyberspace (*i.e.,* what is important to them) changes.

A related problem is the need to maintain situational awareness in cyberspace as a domain unto itself. In the physical world, we strive for a common operational picture to provide commanders with a view of the battle space to support situation assessment, decision making, command and control, and battle damage assessment (*i.e.,* Boyd's OODA loop). As we embrace cyberspace as a domain of operations, we are faced with the following questions: *How do cyber and physical domain operations interact? How do we attack and defend given the speed at which events happen in this domain? Do we need a cyberspace common operational picture, or can cyberspace be merged into the existing physical domain COP? What information is available to support the cyberspace commander, and what information should be available?*

This paper will not attempt to address all of these questions, but the framework we present will help establish necessary relationships among physical and cyberspace entities. Key to our framework is the projection of cyberspace events and concepts into qualia (plural of quale). It is our conjecture that there cannot be a solution to any situational awareness problem without realizing that people and the environment we are sensing with our electronic

and electromagnetic sensors, devices, and networks have to be projected into a representation that allows association between concepts in those respective domains. Therefore, we propose to map everything to qualia. Qualia are the subjective qualities people associate with stimuli and are not reproducible outside the mind of the person experiencing them. People think in qualia space. Therefore they can't be truly aware of the situation unless we generate a "qualiarized" view of situation.

This paper provides a vision of an end state that has not previously been achieved. Our intent is to promote the idea that qualia can improve our situational awareness in cyberspace—and other domains as well. We are currently performing dedicated research to discover how we can implement this framework. As our research reveals specific solutions, we will publish them in future papers.

The rest of the paper is organized as follows. The "Related Work" section provides some background on existing research with qualia concepts. How qualia and their application to the cyberspace awareness problem are discussed in the "Qualia" section. The "Mission Mapping Framework" section presents a framework for mapping missions to cyberspace resources, and the "Cyber Qualia Agents" section introduces the concept of using cyber qualia agents to assist decision makers at all levels in performing their tasks. The "Implementation Challenges" section discusses implementation challenges and other future research ideas, and the "Summary" concludes the paper.

Related Work

There is considerable work in qualia philosophy. However, our belief is that this research centers on the existence (or nonexistence) of qualia, as opposed to how qualia can be applied to solve real world problems. Philosophers like Thomas Nagel [4] and Frank Jackson [5] argue for the existence of qualia while Daniel Dennett, [6] and Paul Churchland [7] are critics.

It is our contention that qualia do indeed exist and that they can be measured, quantified, and used to improve situational awareness. We are less interested in the philosophical arguments over whether qualia do or do not exist than we are in how intelligent beings are able to observe sensory data (sight, sound, touch, *etc.*) and form perceptions and understanding about what is happening in the real world.

In the world of sensors, current technology does not allow us to come up with generalized solutions to problems not previously encountered. While the capabilities of our sensors are constantly improving, we are not significantly increasing our level of situational awareness. Furthermore, adding more sensors and more data tends to make the problem worse.

Conventional approaches to situational awareness assume one can come up with a computer processing approach and associated representation, then take the outputs of that and present it to a human with acceptable results. These approaches have delivered limited success because a human's representation of the world is in the form of qualia, and not in increasingly detailed data sets collected by sensors. The need for an exact replication of the real world is because it is the only way one can ensure a human can qualiarize the situation. An exact replication of the real world in forms not normally sensed by the human operator cannot be easily assimilated by humans, which is why our brains form qualia in the first place. A situational awareness world model that exploits the concept of qualia would therefore improve a human's ability to effectively interact with and understand the world.

Qualia

As discussed earlier, one of the challenges in mapping cyber entities to the physical domain is that people speak different languages—they care about different things depending on their job task and level of authority. The observe-orient-decide-act (OODA) cycle is a useful way of modeling how intelligent beings make decisions. While we all follow the same type of process, the nature of our decisions will change as a function of our own experiences, level of authority, and assigned tasks or objectives.

When presented with the same set of information, commanders and network administrators will see things differently because their world view is different. An operational commander has an experience set that allows him to assimilate and incorporate relevant information into decisions. The fact that a given communications node was destroyed or an asset is malfunctioning simply doesn't make much sense to the commander. Similarly, network administrators know the impact to the network because their experience and job function warrants this knowledge, but does not include the impact to deployed forces and their ability to achieve battle space objectives. It is only when the representations across the entire battle space are compatible that these issues are solved.

This is in essence the very idea of qualia. Simply put, the commander and network administrator (and everyone in between) have different qualia spaces in which they process information to make decisions. Qualia are what allow an intelligent being to experience and recognize a particular sensory input. They represent information in a form the user truly understands, and each being constructs its world model using qualia by mapping what it observes into its own unique qualia space.

Mathematically, qualia are explained as "our internal perception of the basis set we use to represent the variety of stimuli we encounter." [8] Further, "this basis set allows the representation of the infinite variety of stimuli we sense into a small number of clusters, qualia, of relevant things." [8] It is believed that the infinite varieties of stimuli observed in the physical world are represented as qualia. Likewise, we believe it is possible to extend this concept into cyberspace.

Cyberspace is filled with raw data that is meaningless to many users who need alternative representations of that data. What is needed is a way to shape, filter, and present the data to decision makers (which could be people or automated tools) in the form that is most useful for making decisions in a timely manner.

Mission Mapping Framework

Our framework uses a multilayer graph model (see Figure 1) to capture relationships (an example of qualia of qualia, or compound qualia) horizontally and vertically between individual entities. Each layer depicts the relationships (compound qualia) among missions, business processes, organizations, people, systems, *etc.* Each of these concepts (mission, business processes, *etc.*) is a quale that could be important to someone. This framework is not limited to only these layers. The number of layers and the information being captured in each layer depend on the problem to be addressed. The layers identified here are appropriate for capturing the relationships between a military mission and the physical network. Interlayer mappings address the interdependent relationships that allow correlation of abstract concepts, such as aligning mission/process effectiveness with underlying network performance.

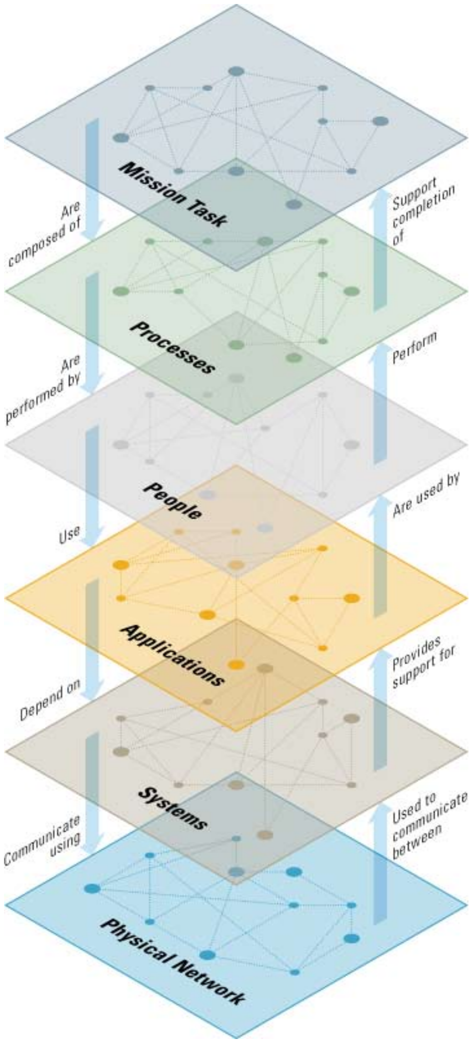


Figure 1 Map and Mission Context

With these associations, commanders and support personnel can determine how operational tasks and missions are affected by network or system outages. As shown later, this framework supports the development of cyberspace situational awareness for commanders who need to understand how cyber and physical domain operations support and complement each other, universal situational awareness.

Cyber Qualia Agents

The things we care about in cyberspace (radio transmissions, network traffic flows, user behavior, *etc.*) are manmade. It is reasonable then to assert that we can use cyber qualia agents to understand the status, state, and location of cyber entities plus their qualia (relationships) and impact on the mission. These software agents will capture and present information in the appropriate qualia spaces for decision makers at all levels.

We begin with the notion of self-aware cyber qualia agents that analyze cyber entities. A cyber entity is an instantiation of a specific concept of something in cyberspace. Cyber concepts are composed of other cyber concepts. These concepts can be programs or services (web servers and email servers for example), security devices (firewalls, intrusion detection systems, *etc.*), and malicious code. Cyber concepts can also be events and other things (response times, denial of service attacks, human intent, *etc.*) that decision makers might want to know about (detect, distinguish and characterize).

Cyber concepts are characterized by a set of attributes or properties, as shown in Figure 2. Cyber concepts are not unique to individual entities, though the qualia representation of a concept may be unique to each individual entity. For example, several entities may sense the concept of an email client, but a qualia representation will be unique to a particular entity or instance of a concept.

One would like to believe that each and every concept is detectable, distinguishable, and characterizable by a finite set of properties or attributes.

Unfortunately, many (if not all) concepts that we wish to detect, distinguish, and characterize cannot be uniquely categorized by a simple set of attributes that would allow us to completely label that concept. In fact, it is a very difficult problem to distinguish one concept from another. For example, the many concepts, which are themselves qualia, that we would call a successful result of a cyber attack probably couldn't be defined or listed. That result, the successful cyber attack, which is something new to us, is a quale. Every network administrator would agree that it was a successful attack when explained to them. Even if we could list all the concepts of every known successful attack, the list would immediately become obsolete as new attacks are created every day. What makes something a successful attack is so varied that prior attempts to capture the concept have resulted in fragile solutions that have only limited abilities. That same idea must be extended to the definition of all the aspects of the environment to allow the generation of a real useful world model.

We propose that it is only through a universal representation that captures the variability of the environment into a useful world model, for example the use of qualia, across all the various levels of the cyber hierarchy, that the cyber situation can be captured. We believe it a mistake to think we can, *via* definition, capture what we mean when we use a term limited to some list of attributes for its definition to refer to an entity. In fact, that fails to capture the real variability of the entity when we use those same terms.

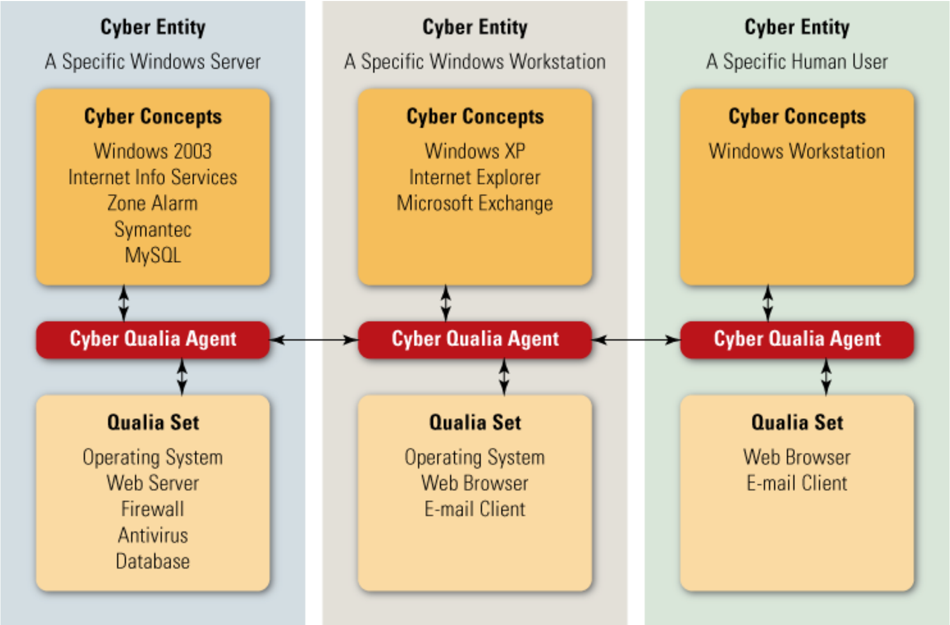


Figure 2 Cyber Concept Relationship Diagram

We have asserted that cyber concepts are themselves qualia, and there exist qualia of qualia. We call these relationships compound qualia. Therefore, cyber concepts have qualia associated with them (overtaxed central processing unit [CPU], unused memory, excess bandwidth, *etc.*) and it is this compounding of qualia that actually provides meaningful information to the human, increasing his awareness of cyberspace. Compound qualia must be learned by continuous observation of the entities by the cyber qualia agents. A general purpose method for learning has not yet been defined. We only acknowledge that it must occur along with a set of processes that manipulate the resulting representation to capture an accurate representation of an entity.

One of the keys to our framework is that a cyber qualia agent is self-aware. In this model, we believe that there are no mystical aspects of the computation of self. It is just another quale that we expect will be required for cyber qualia agents to present information into an entity's qualia space. Cyber qualia agents are not only aware of themselves (this includes the ability to know what they themselves consist of and what they are processing and how they are processing those measurements, *i.e.,* thinking), but they are also aware of other cyber qualia agents. Furthermore, an agent's awareness is extended to the cyber entity to which it is assigned.

When an agent is first started, it learns about itself and its surroundings by sensing the entity to which it is associated and monitoring the cyber concepts associated with that entity. This learning process is a universal approach to gathering environmental information. This is a very important point that warrants extra emphasis. All levels of our framework use the same processing function. They learn. Cyber qualia agents begin with little or no knowledge of the environment. They utilize generic cyber sensors to learn about the environment and what is taking place inside of it. Qualia agents extract the qualia representation without being told what it is. However, we allow the possibility of "teaching" a cyber qualia agent a set of facts that the qualia agent would not be required to learn. For example, a particular manufacturer may pre-program their cyber qualia agents with basic facts about their cyber entities. This is consistent with humans in that we all have genetic predispositions for certain characteristics or abilities.

To facilitate efficient communications, cyber qualia agents organize themselves so that information can be shared as necessary. Certain qualia agents are responsible for propagating pertinent information. For example, a user of a system is itself an entity and the cyber qualia agent associated with that specific human has the task of interfacing with the qualia space of that human. Qualia agents do not simply pass along data to the user, but instead present information into its representation of the user's qualia space, enhancing the user's situational awareness. The idea is that a self-adapting agent "learns" what that human uses and thus adapts its qualia representation to optimize interfacing to that human. In this manner, information is presented to the human user in the "language" that he understands and is able to act upon.

Cyber qualia agents perform situation assessment, assisting the user in achieving situation awareness. The concept of self is temporal. Cyber qualia agents must constantly monitor their entities to ensure an accurate representation exists in the user's qualia space.

Implementation Challenges

We believe this framework will work well for achieving situational awareness in cyberspace, but it is not limited to that domain. It can be extended to any domain where entities need to be monitored and a cyber agent can be associated with that entity. Therefore, this framework can be used to monitor not only cyberspace entities, but also space, air, land, and sea entities. The ability to monitor these domains with a general, extensible framework provides a decision maker with a truly integrated battlespace situational awareness. Our goal is to attain universal situational awareness, thus being able to represent everything physical and cyber with a single framework using qualia agents.

Admittedly, there are many challenges to overcome before this framework can become a reality. The method by which cyber qualia agents communicate is one. Cyber qualia agents cannot be constrained to a limited vocabulary. In fact, the vocabulary is the learned qualia for that entity. Neither can they be forced to communicate through a centralized server. They must be aware of other cyber qualia agents and communicate with them efficiently. Cyber qualia agents will communicate using a language that represents each entity's qualia space. It is the set of qualia each entity possesses that is important in the communication with other qualia agents.

As stated earlier, our cyber qualia agents must be self-aware. They must be able to monitor and observe the qualia associated with their entity, determine the intent of the entity, and present information to the entity that improves its situational awareness. Cyber qualia agents are all created equal. They differ in that they learn about their environment, and themselves, through the sensing and monitoring of cyber entities. Creating a generic qualia agent that can learn will certainly be a challenge. It requires a breakthrough in technology that we have not yet seen. Yet, it is this generic qualia agent that will change the way we solve problems previously unsolvable. We will no longer be required to identify what something "bad" looks like. Cyber qualia agents will learn what is bad and react accordingly.

Summary

This article presents a framework for awareness in cyberspace. It provides a means for determining the actual cyber entities used to perform a specific mission by associating cyber concepts with the systems that use them. It also provides a means for monitoring cyber entities and improving a particular entity's situational awareness of cyberspace by using cyber qualia agents to provide pertinent information as needed.

Many challenges stand in the way of implementing this framework. However, technological advances in recent years allow us to pursue this idea. A truly integrated view of not only cyberspace, but of the entire Battlespace is possible.

Acknowledgements

Special thanks go to the QUEST (QUalia Exploitation of Sensor Technology) discussion group for their innovative ideas and insightful discussions. The group includes Dr. Matthew Kabrisky, Dr. Mark Oxley, Dr. Kenneth Bauer, Adam S. Rogers, and 1st Lt Stephen Mott. Additionally, we thank the reviewers for their constructive and insightful comments.

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the US Government.

References

1. Department of Defense. National Military Strategy for Cyberspace Operations (NMS-CO) (TANK-approved draft). Version 6.0. Washington: DoD. 25 August 2006.
2. M. Gettle, "Air Force releases new mission statement," *Air Force Print News,* http://www.af.mil/news/story.asp?storyID=123013440, last accessed 12 October 2006.
3. Stanley, J.E.; Mills, R.F.; Raines, R.A.; Baldwin, R.O., "Correlating network services with operational mission impact," *Military Communications Conference, 2005. MILCOM 2005. IEEE,* vol., no., pp. 162-168 Vol. 1, 17-20 Oct. 2005.
4. T. Nagel. "What is it like to be a bat?" *The philosophical Review,* October 1974.
5. F. Jackson. "Epiphenomenal Qualia," *Philosophical Quarterly,* 32: 127-136, 1982.
6. D. Dennett. *Consciousness Explained.* Little, Brown and Co., Boston, 1991.
7. P. Churchland. "Knowing Qualia: A Reply to Jackson", in A Neurocomputational Perspective: The Nature of Mind and the Structure of Science, 1989.
8. Rogers, S. K., Kabrisky, M., Bauer, K., and Oxley, M. "Computing Machinery and Intelligence Amplification," *Computational Intelligence, The Experts Speak* (Chapter 3), New Jersey: IEEE Press, 2003.

About the Authors

Timothy H. Lacey | is an instructor of computer science in the Department of Electrical and Computer Engineering at the US Air Force Institute of Technology, Wright-Patterson AFB. Mr. Lacey has a BS in computer science/management of computer information systems from Park College and an MS in computer systems from AFIT. He teaches and conducts research in both network and software security. Contact him at timothy.lacey.ctr@afit.edu.

Dr. Robert F. Mills | is an assistant professor of Electrical Engineering in the Department of Electrical and Computer Engineering at AFIT. Dr. Mills received a BS degree in Electrical Engineering from Montana State University, an MS degree in Electrical Engineering from AFIT, and a PhD in Electrical Engineering from the University of Kansas. His research interests include communications systems, signal detection and exploitation, network security/management, and cyber operations and warfare.

Dr. Richard A. Raines | is the Director of the Center for Cyberspace Research at AFIT. Dr. Raines holds a BS degree in Electrical Engineering from the Florida State

University, an MS in Computer Engineering from AFIT, and a PhD in Electrical Engineering from Virginia Tech. He teaches and conducts research in information security and global communications.

Major Paul D. Williams, PhD USAF | Major Williams earned his BS from the University of Washington, his MS from the Air Force Institute of Technology, and his PhD from Purdue University. He is an Assistant Professor of Computer Science and Cyber Operations in the Department of Electrical and Computer Engineering at the Air Force Institute of Technology, Wright-Patterson AFB, Ohio. He has served in many information operations roles, both operational and supporting, for seventeen years. His research interests center on cyber warfare, and include algorithms, artificial intelligence, and security-focused computer architectures.

Dr. Steven K. Rogers | is a Senior Scientist at the Air Force Research Laboratory. He serves as the principle scientific authority for Automatic Target Recognition and Sensor Fusion. Dr Rogers' research focuses on qualia exploitation of sensor technology, QUEST.

IATAC SPOTLIGHT ON EDUCATION

Idaho State University

by Ron Ritchey

The Idaho State University (ISU) Informatics Research Institute (IRI) [1] and Department of Computer Information Systems (CIS) in the College of Business [2] provide students with a sound foundation in business, information systems, and computer science principles. Students learn methods and techniques for developing secure information systems while gaining an understanding of how organizations conduct and manage business. The CIS department serves as the official administrative home of the CIS degree, whereas the IRI houses the Information Assurance Program (IAP) [3] and National Information Assurance Training and Education Center (NIATEC). [4]

The program offers BBA and MBA degrees in Computer Information Systems (CIS). Students enrolled in the CIS program may take advantage of concentrations in security that the IAP offers. The IAP gives students a solid foundation in security, offering an interdisciplinary program blending technology; policy and practice; and awareness, education, and training principles. The IAP ensures that students will be conversant in various industry-recognized knowledge bases, including those from the Committee on National Security Systems (CNSS) and the International Information Systems Security Certification Consortium ([ISC]2).

Early in their program of study, all students are required to complete CompTIA's Security+ examination to document their basic knowledge of technology. Although the program of instruction is based on the CNSS curriculum, students are expected to meet other professional standards. After the first year, students are required to complete the (ISC)2 Systems Security Certified Professional (SSCP) examination, whereas graduate students are required to complete the Certified Information Systems Security Professional (CISSP) examination. A majority of IAP students participate in the Federal Cyber Service Scholarship for Service program, in which ISU is one of the few schools offering an MBA program. From its inception, the IAP had a 100% placement rate, with up to four offers for each student.

The IRI at ISU also hosts the NIATEC, a consortium of academic, industry, and government organizations working to improve literacy, awareness, education, and training standards in information assurance (IA). Directed by Dr. Corey Schou, NIATEC develops curriculum materials that are freely available. NIATEC is a culmination of efforts resulting from the National Institute of Standards and Technology's (NIST) and National Security Agency's (NSA) requests back in 1992 to establish a clearinghouse for IA curriculum materials. NIATEC offers materials for general high-level IA education and for specific topics. For example, universities have access to 8,000 pages of instructional material about IA from the designated approving authority's (DAA) perspective. NIATEC also offers short courses regarding NIST Special Publication (SP) 800-37, Guide for Security Certification and Accreditation of Federal Information Systems. Currently, NIATEC is finalizing a series of 10-minute modules on cryptography and another on forensics. By providing materials at high and low levels and breaking topics into short modules, educators have the option of building an entire course or integrating the material into existing curricula. ■

References

1. More information about the IRI can be found at *http://iri.isu.edu*
2. More information about the CIS department can be found at *http://cob.isu.edu/cis/cishome.aspx*
3. More information about the IAP can be found at *http://security.isu.edu*
4. More information about NIATEC can be found at *http://niatec.info*

US-CERT: America's Cyber Watch and Warning Center

by the Department of Homeland Security
Office of Cybersecurity and Communications
National Cyber Security Division
United States Computer Emergency Readiness Team (US-CERT)

PUBLIC "-//W3C//DTD
xmlns="http://www.w3.org/1999/xhtml"><
http-equiv="Content-Type" conte
InstanceBeginEditable name=
tle" --> <title>IATAC - Information Assuran
="text/css" />
pt type="text/javascript">function MM_op
dow.open(theURL,winName,features);
name="head" --><!-
-//W3C//DTD XHTML
w3.org/1999/xhtml"><
"Content-Type" conte
le name=
Information Assura
MM_op
US-CERT

The Department of Homeland Security protects our nation's critical infrastructure from physical and cyber threats. Cyberspace has united once distinct information infrastructures, including our business and government operations, our emergency preparedness communications, and our critical digital and process control systems and infrastructures. Protecting these systems is essential to the resilience and reliability of the nation's critical infrastructures and key resources and, therefore, to our economic and national security.

The Department's cyber security division created the United States Computer Emergency Readiness Team (US-CERT) in September 2003 to protect the nation's Internet infrastructure by coordinating defense against and response to cyber attacks. US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

US-CERT collaborates with federal agencies, the private sector, the research community, state and local governments, and international entities. By analyzing incidents that these entities report and coordinating with national security incident response centers responding to incidents on classified and unclassified systems, US-CERT disseminates reasoned and actionable cyber security information to the public.

To protect America's cyberspace, US-CERT—

- Maintains a 24x7 secure operations center
- Established a public Web site (*http://www.us-cert.gov*) to provide the public with cyber-related information
- Acts as a trusted third-party to assist in the responsible disclosure of vulnerabilities
- Develops and participates in regional, national, and international level exercises
- Supports forensic investigations with recursive analysis on artifacts
- Provides malware analytic and recovery support for government agencies
- Provides behavior techniques for dynamic and static analysis
- Manages the malicious code submission and collection program
- Disseminates emerging cyber threat warnings
- Administers the National Cyber Alert System to disseminate cyber security information to all Americans
- Provides fused, current, and predictive cyber analysis based on situational reporting
- Provides onsite incident response capabilities to federal and state agencies
- Supports ongoing federal law enforcement investigations
- Coordinates federal programs of CERT and Chief Information Security Officer (CISO) peer groups for sharing incident information, best practices, and other cyber security information
- Collaborates with domestic and international computer security incident response teams.

Building Success Through Relationships

US-CERT is expanding its operations through partnerships with the private sector security vendors, academia, federal agencies, information sharing and analysis centers (ISAC), state and local governments, and domestic and international organizations. US-CERT participates in various information-sharing venues, including leveraging ISACs and engaging with corporate computer security incident response teams.

US-CERT plays an integral role in helping develop regional programs, such as the South East Cyber Anti-Terrorism and Security (SECATS) located on the Gulf Coast, as well as the Puget Sound Partnership for Cyber Security located in the Pacific Northwest. Stakeholders developed these regional efforts, made up of government, private, state, and local entities, as an information-sharing mechanism.

US-CERT Programs and Initiatives

US-CERT has established several important components that foster and facilitate information sharing and collaboration on

cyber security issues among government, industry, academia, and international entities.

Examples of current collaboration efforts are as follows—

- **US-CERT website**—Provides government, private sector, and the public with information needed to improve its ability to protect information systems and infrastructures. The Web site includes information about current activity, events, resources, publications, affiliates, and more.
- **National Cyber Alert System**—Delivers targeted, timely, and actionable information to Americans, educating them on how to secure their own computer systems.
- **National Cyber Response Coordination Group (NCRCG)**—Established in partnership with the Department of Defense and the Department of Justice, NCRCG serves as the federal government's principal interagency mechanism to facilitate coordination of efforts to respond to and recover from cyber incidents of national significance.
- **US-CERT Portal**—Provides a secure Web-based collaborative system to share sensitive cyber-related information with government and industry members.
- **Government Forum of Incident Response Security Teams (GFIRST)**—A community of more than 50 incident response teams from various federal agencies working together to secure the federal government.
- **Chief Information Security Officers (CISO) Forum**—A community of more than 50 CISOs from small, medium, and large federal departments/agencies.
- **US-CERT Einstein Program**—An automated process for collecting, correlating, analyzing, and sharing computer security information across the federal government to improve our nation's cyber situational awareness.
- **Internet Health Service**—A service that provides information about Internet activity to federal government agencies through the GFIRST community.

Participation Is Key to Improving Cyber Security

You can be an informed citizen by signing up to receive free alerts and important cyber security information. Register on the US-CERT website at *http://www.us-cert.gov/cas/signup.html*. ■

Report Cyber Incidents, Vulnerabilities, and Phishing Scams

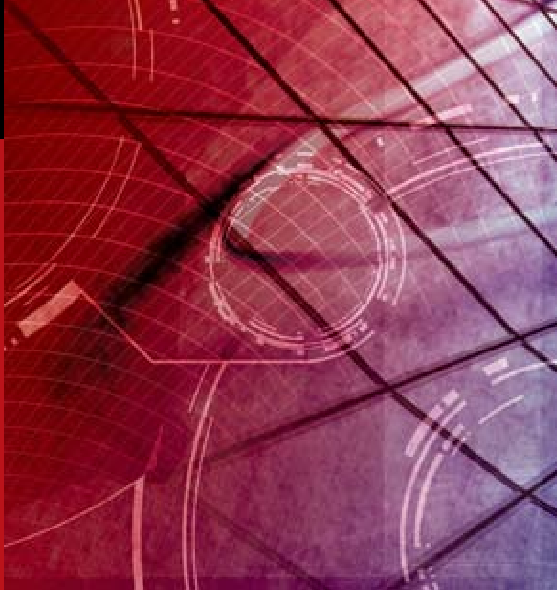
US-CERT encourages you to report any suspicious activity, including cyber security incidents, possible malicious code, vulnerabilities, and phishing related scams. Reporting forms can be found on our homepage at *http://www.us-cert.gov*. You can also submit cyber threats as follows:

Phone:	888/282-0870
Fax:	703/235-5965
Email:	soc@us-cert.gov (in the clear and encrypted)

Obtaining Additional Information

To learn more about US-CERT,
visit or contact:

http://www.us-cert.gov
info@us-cert.gov



Executing the CND Data Strategy within the NetOps Community of Interest

by Larry Frank

The Department of Defense (DoD) Computer Network Defense (CND) Architect is responsible for developing and implementing the CND operational Architecture. In this role, the CND Architect chairs the CND Architecture Working Group (CAWG). The CND Architect has coordinated CND community input into the information assurance (IA) component of the Global Information Grid (GIG) architecture and the Joint NetOps architecture, and it has then facilitated the synchronization of the IA and NetOps architectures. This effort enables these two communities to provide consolidated architecture inputs into the Version 1.2 update of the Net-Centric Operations and Warfare Reference Model (NCOW-RM).

In examining the way CND is conducted within DoD, the CAWG identified numerous issues that must be resolved if the future CND architecture is to execute effective defense of the Net-Centric GIG. The current solutions for CND are product focused, creating an environment in which information is highly fragmented and locked inside proprietary data schemes. Integrating these products requires resource-intensive, point-to-point solutions that make the environment brittle and expensive to develop and maintain. In a worst case, every product must interact with every other product, creating a situation resembling the one that Figure 1 illustrates.

In this context, CND is not different from any other warfighting or business

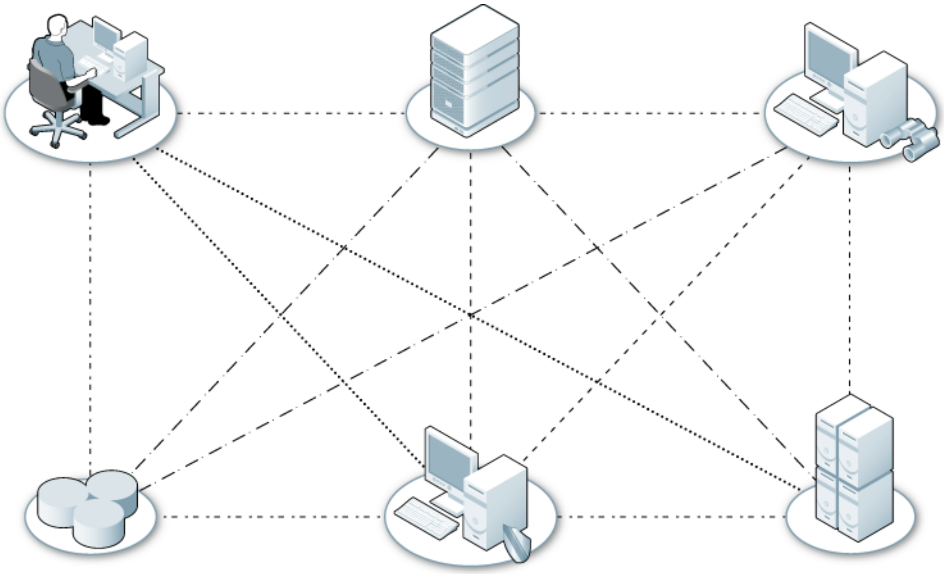


Figure 1 Point to Point Integration

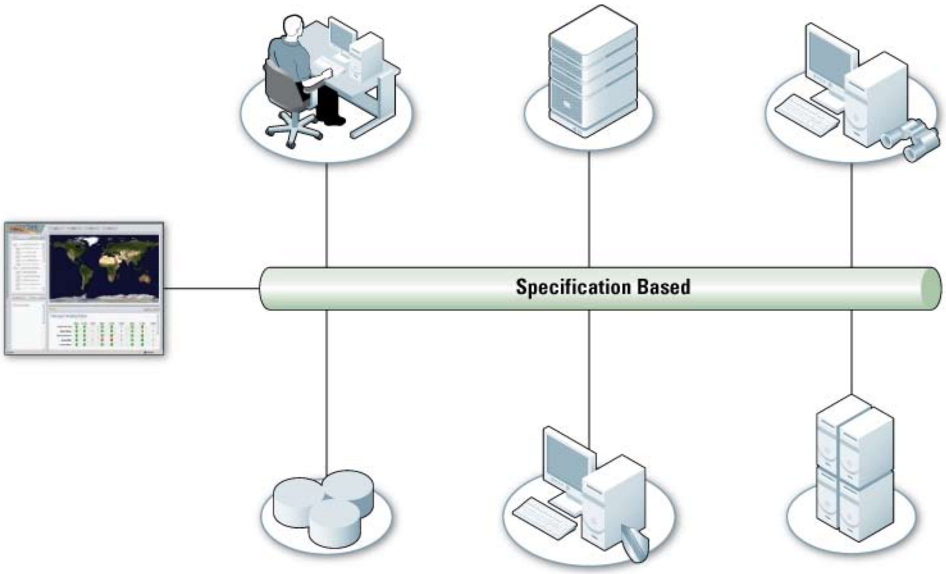


Figure 2 Net-Centric Model

system. The current industry model for overcoming the problems inherent in the point-to-point engineering model is a service-oriented architecture. For DoD, this means transforming CND so that it can operate using Net-Centric concepts. In a Net-Centric model, the above integration would resemble Figure 2.

One step for transforming CND to this operating model requires the development of data standards. At the February 2006 DoD IA Workshop, the CND Architect presented a strawman CND data model (OV-7 in terms of DoD architecture framework) (see Figure 3) to be used as a basis for the initial discussion of implementing DoD data strategy requirements within the CND operational environment.

As DoDD 8320.2 envisioned, each community will create and register the semantic and structural meta-data for community data into the DoD meta-data registry. Authorized entities inside and outside the community will then be able to understand the data when it is exposed *via* services.

The original data model, created at a high level, was completely CND centric. However, as the CAWG moved to coordinate the strawman for approval within the working group, it became clear that most data sets CND force need to have true situational awareness belonging to communities outside CND. Realizing that the US Strategic Command (USSTRATCOM) had stood up the NetOps community of interest (COI), the CAWG considered it prudent to frame CND data in the context of the larger, more encompassing NetOps framework. Figure 4 illustrates this model.

The original CND model had used "CND situation awareness data" as the parent of the decomposition. Because the Joint NetOps architecture had referred to "NetOps data" as an all-encompassing term, the new model used that as the parent. The model decomposes NetOps data into three essential tasks: GIG enterprise management, GIG content management, and GIG network defense. Data shared among these tasks and data required from outside NetOps would be included. It was hoped that segmenting

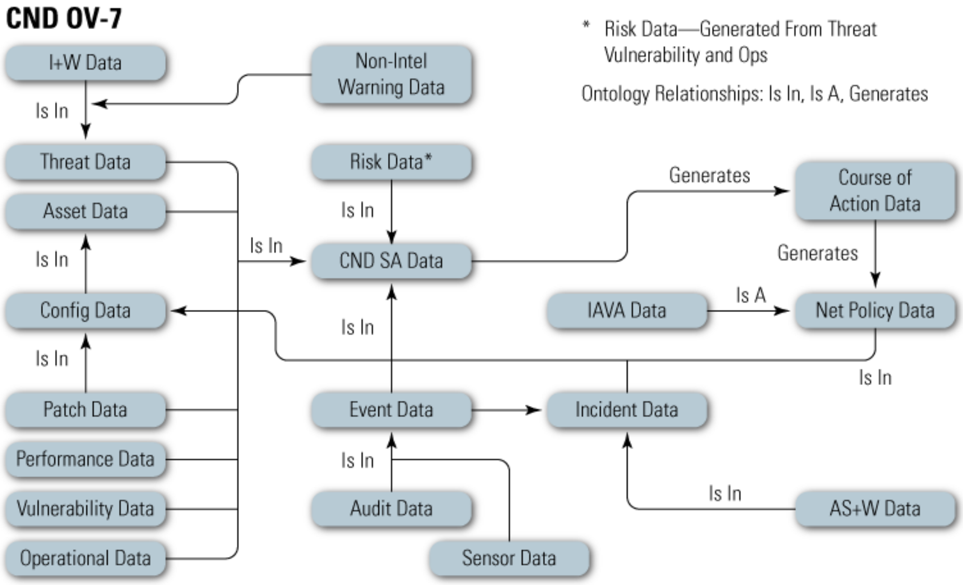


Figure 3 Original CND OV-7

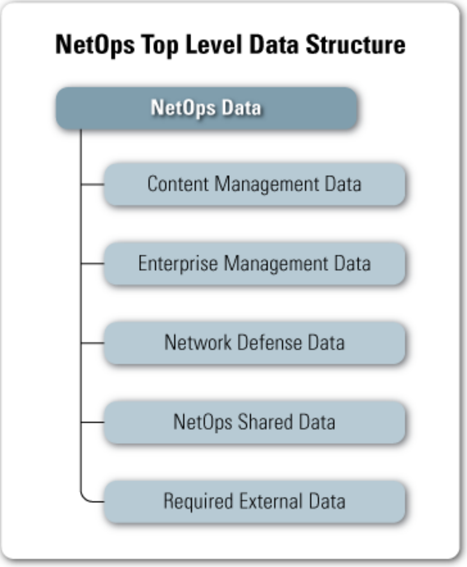
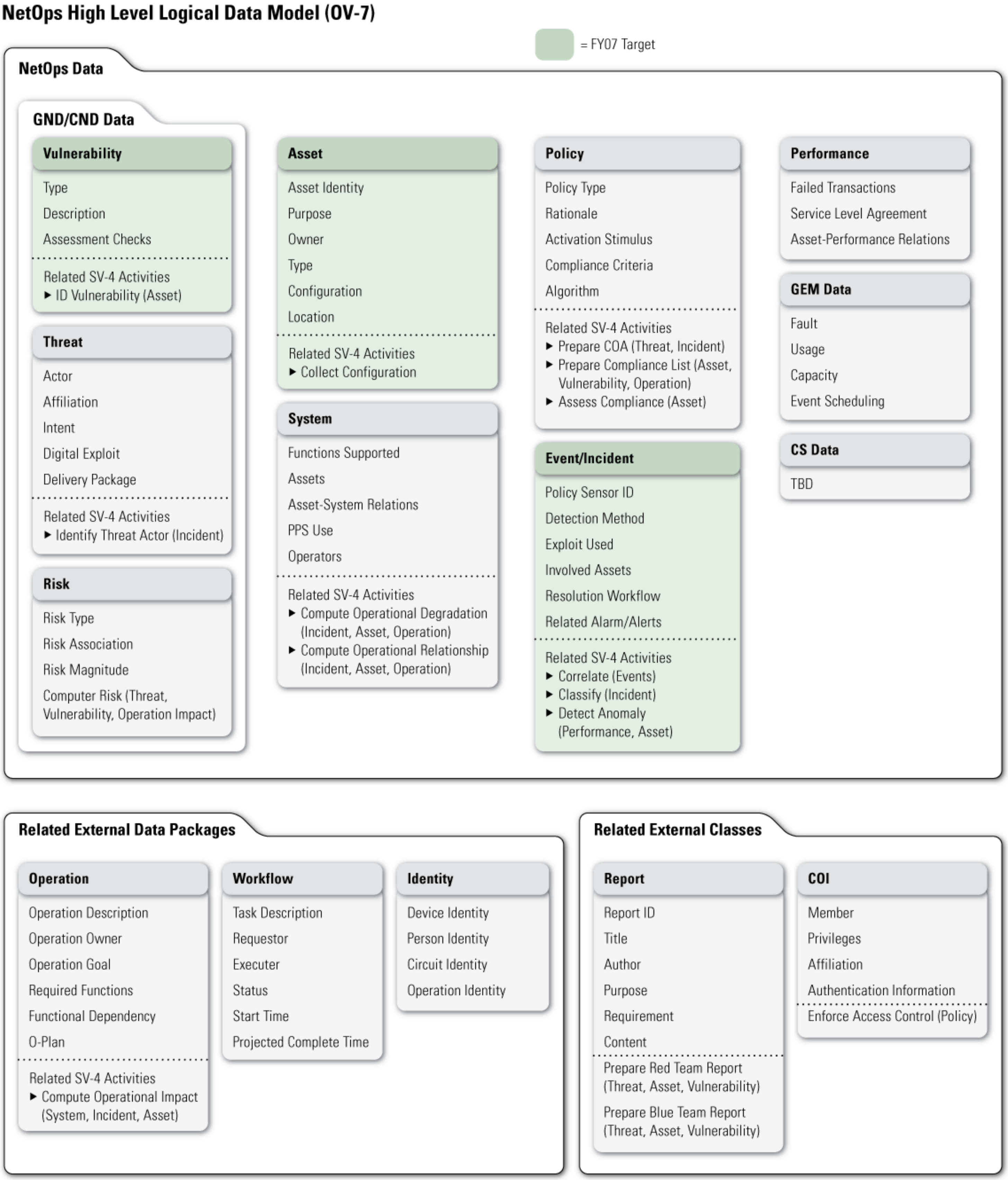


Figure 4 Top-Level NetOps Data Model



NetOps High Level Logical Data Model (OV-7)

🟩 = FY07 Target

NetOps Data

GND/CND Data

Vulnerability
- Type
- Description
- Assessment Checks

Related SV-4 Activities
- ▶ ID Vulnerability (Asset)

Threat
- Actor
- Affiliation
- Intent
- Digital Exploit
- Delivery Package

Related SV-4 Activities
- ▶ Identify Threat Actor (Incident)

Risk
- Risk Type
- Risk Association
- Risk Magnitude
- Computer Risk (Threat, Vulnerability, Operation Impact)

Asset
- Asset Identity
- Purpose
- Owner
- Type
- Configuration
- Location

Related SV-4 Activities
- ▶ Collect Configuration

System
- Functions Supported
- Assets
- Asset-System Relations
- PPS Use
- Operators

Related SV-4 Activities
- ▶ Compute Operational Degradation (Incident, Asset, Operation)
- ▶ Compute Operational Relationship (Incident, Asset, Operation)

Policy
- Policy Type
- Rationale
- Activation Stimulus
- Compliance Criteria
- Algorithm

Related SV-4 Activities
- ▶ Prepare COA (Threat, Incident)
- ▶ Prepare Compliance List (Asset, Vulnerability, Operation)
- ▶ Assess Compliance (Asset)

Event/Incident
- Policy Sensor ID
- Detection Method
- Exploit Used
- Involved Assets
- Resolution Workflow
- Related Alarm/Alerts

Related SV-4 Activities
- ▶ Correlate (Events)
- ▶ Classify (Incident)
- ▶ Detect Anomaly (Performance, Asset)

Performance
- Failed Transactions
- Service Level Agreement
- Asset-Performance Relations

GEM Data
- Fault
- Usage
- Capacity
- Event Scheduling

CS Data
- TBD

Related External Data Packages

Operation
- Operation Description
- Operation Owner
- Operation Goal
- Required Functions
- Functional Dependency
- O-Plan

Related SV-4 Activities
- ▶ Compute Operational Impact (System, Incident, Asset)

Workflow
- Task Description
- Requestor
- Executer
- Status
- Start Time
- Projected Complete Time

Identity
- Device Identity
- Person Identity
- Circuit Identity
- Operation Identity

Related External Classes

Report
- Report ID
- Title
- Author
- Purpose
- Requirement
- Content

Prepare Red Team Report (Threat, Asset, Vulnerability)

Prepare Blue Team Report (Threat, Asset, Vulnerability)

COI
- Member
- Privileges
- Affiliation
- Authentication Information

Enforce Access Control (Policy)

Figure 5 Expanded NetOps Data Model

Element	Description	JCD	IDMEF (Notes 1, 2, and 4)
Event Elements			
Event Name	Name of the event associated with an incident	event_name	ClassificationReferenceName
Event Category	Category of event		
Event Description	Description of event		
Vulnerability ID	Vulnerability associated with event	vulnerability_id	ClassificationReferenceOrigin
Method of Attack	Name of exploit	exploit	
Collection Method	Device or technique used to collect event	collection_method	AnalyzerProcess
Event Detection Time			DetectTime
Event GMT Start Time	The "Greenwich Mean Time" or Zulu date and time the source initiated a connection to the targeted information system	gmt_start_date	(Alert|ToolAlert|CorrelationAlert|OverflowAlert).CreateTime

Table 1 Extract of Event Data Matrix

the data model in this manner would provide a framework for the CND community in which it could work and would foster integration when the NetOps COI began developing its data standards. At a minimum, it allowed the CND community to articulate which communities should take responsibility for defining the semantic and structural meta-data needed for Net-Centric operations.

Once the top-level data model was developed, the CAWG focused on providing greater detail. At a high level, the CAWG mapped the original OV-7 data sets into the data model shown in Figure 5. Data sets (shown in green), asset and event/incident from the NetOps shared data set, and vulnerability data from the network defense data set are the data sets needed for the CND pilot of a Net-Centric implementation, scheduled for delivery in fall 2007.

Once the CAWG had agreed on a high-level data structure, the CND Architect chartered the NSA CND Research and Technology Program Management Office (CND R+T PMO) to begin detailed defining associated data sets, starting with the three required for the pilot. Meanwhile, the CND Architect has been working to socialize the above model within the NetOps COI to ensure that the work being performed under CAWG was acceptable to NetOps COI and moves the entire community toward the Net-Centric vision.

The CND R+T PMO has established a process for formulating the proposed semantic and structural meta-data. This process captures data definitions from known systems that appear to have associated data, reviews literature to identify commercial standard data models, and maps collected information into a matrix. Table 1 shows an extract of one of these event data matrices. The PMO team uses the map to create a unified modeling language (UML) data package that incorporates the analysis results. Figure 6 illustrates an initial draft for the event data type.

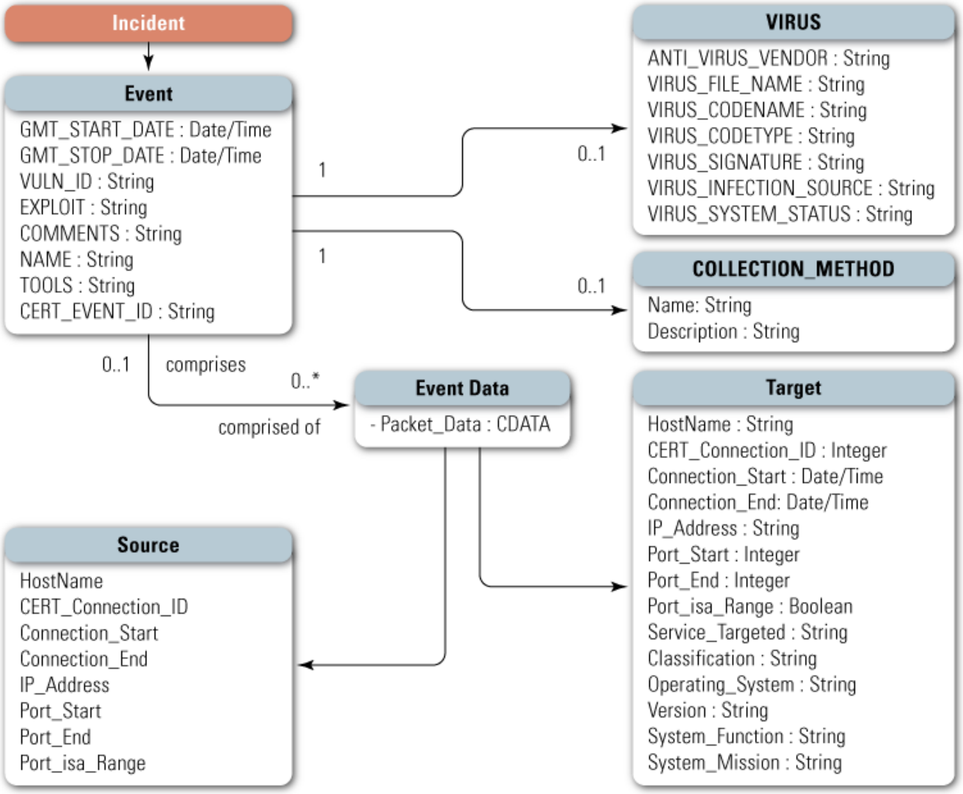


Figure 6 UML Depiction of Event

The development and implementation of a Net-Centric data strategy is a necessary step in transforming any environment from a product-centric to a Net-Centric model.

This work is ongoing. The CND R+T PMO is only now delivering drafts for the asset, incident/event and vulnerability models to CAWG for review. The models must be translated into eXtensible markup Language (XML) before being registered with the DoD Meta Data Registry. Because assets and incident/events are in shared space, the CAWG will seek input from the broader NetOps COI, which recently reestablished its data working group, to ensure concurrence from the wider NetOps community. Simultaneously, the CAWG is researching external COIs to identify existing standards for information in related external data packages and classes to capitalize on existing standards.

The development and implementation of a Net-Centric data strategy is a necessary step in transforming any environment from a product-centric to a Net-Centric model. The CAWG invites inputs from related working groups in the CND data model development, and it hopes that the CAWG experience demonstrated in this task will help other COIs as they take this journey. ■

About the Author

Larry Frank | is a contractor supporting the CND Architect, coordinating the efforts of groups operating under the CND Architecture Working Group. His last position prior to retiring from the Army in October 2000 was the Director of Operations (J-3) for the Joint Task Force-Computer Network Defense.

CONFERENCES

8th IEEE Information Assurance Workshop

The 8th IEEE IAW was held at the Thayer Hotel at the US Military Academy in West Point, NY, from 20–22 June 2007. The conference featured cutting-edge information assurance (IA) research from all over the globe presented by academic institutions and researchers. The Information Technology and Operations Center (ITOC) and the Department of Electrical Engineering and Computer Science from the US Military Academy organized and hosted the event, which the IEEE Systems, Man, and Cybernetics (SMC) Society and the National Security Agency (NSA) sponsored. Some institutes of higher learning that participated included the Naval Post Graduate School, the Air Force Institute of Technology, Georgia State University, Virginia Tech University, Carnegie Mellon University, Mississippi State University, and the University of Toledo. Information Assurance Technology Analysis Center (IATAC) reviews IA technologies, such as those presented at this conference, to explore emerging IA technologies several years before they become commercially available.

The papers presented at the conference covered IA professional development, IA best practices, security considerations, computer forensics, wireless security, honeynets, privacy, intrusion, secure software technology, and information warfare. A 51-person program committee reviewed the 48 submissions and selected *A Linux Implementation of Temporal Access Controls* by Cynthia Irvine, Thuy Nguyen, and Ken Chiang as the best paper. Conference proceedings can be ordered from *http://www.ieee.org*.

The Director of the Department of Defense (DoD) Public Key Infrastructure (PKI) Program Management Office (PMO) at NSA gave the keynote address on DoD's ongoing PKI efforts. Tom Cross, a member of IBM Internet Security System's X-Force Advanced Research Team, spoke about hackers, countercultures, and their relationship to mainstream society. Pieter Mudge Zatko, leader of the hacker think tank "L0pht" and currently the Division Scientist for BBN Technologies, discussed security vulnerabilities. Randy Marchany, Director of Virginia Tech's IT Security Laboratory, spoke about the progress (or apparent lack thereof) the IA community has made in the past two decades. Adam Laurie, Director of Bunker Secure Hosting Ltd., spoke about the current and future uses of radio frequency identification (RFID) and the vulnerabilities inherent in the technology.

Please check the IEEE IAW website, *http://www.itoc.usma.edu/workshop*, for more information about next year's conference. ■

Dr. Corey Schou

by Ron Ritchey

This article continues our series in which we profile members of the IATAC Subject Matter Expert (SME) program. The SME profiled in this article is Dr. Corey Schou, who has been University Professor of Informatics at the Idaho State University (ISU) College of Business (COB) since 2003. Earlier, he served for 16 years as the Chair, CIS program. He is now Associate Dean of Information Systems at ISU. Dr. Schou's research interests are in information security, privacy, and ethics.

Dr. Schou received a PhD in International Law from Florida State University. Earning his PhD before the widespread availability of information systems programs at universities, his law background has given him unique analytical insight into the information systems field. Dr. Schou has more than 30 years of experience in information technology. He has designed and developed systems for various organizations (*e.g.,* Microsoft, Apple and FedEx), including responsibility for designing pilot training systems. After completing his PhD, much of Dr. Schou's research focused on how to effectively implement distance education.

In the early 1990s, Dr. Schou's research established the underlying database for the materials for National Institute of Standards and Technology (NIST) Special Publication (SP) 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model, and for the Committee on National Security Systems (CNSS) standards 4011 through 4016, which are the basis for the IAP curriculum. Dr. Schou's research was integral to the development of the International Information Systems Security Certification Consortium ([ISC]2) [1] Common Body of Knowledge (CBK).

Dr. Schou serves as Director, National Information Assurance Training and Education Center (NIATEC), [2] which develops freely available IA curriculum materials. Under his leadership at NIATEC and ISU's Information Assurance Program (IAP), [3] ISU was designated a National Center of Excellence in Information Assurance Education (NCEIAA).

Dr. Schou is Chair, Colloquium for Information Systems Security Education (CISSE), [4] that brings together industry, government, and academia to work on the shared needs of IA training and education. CISSE also cooperates heavily with the Department of Homeland Security's Software Assurance Workforce Education and Training working group.

Dr. Schou is now the Vice Chairman of the (ISC)2 Board of Directors. He was the first recipient of the (ISC)2 Tipton award for his outstanding contribution to the computer security discipline. In 1996, the Federal Information Systems Security Educators Association (FISSEA) named him Educator of the Year, and he was the recipient of the Information Systems Security Association (ISSA) service award.

He is the author of numerous articles, book chapters, and papers. The subject of his first book was cryptography. His second book, Information Assurance for the Enterprise A Roadmap to Information Security, deals with security architecture and design issues.

If you have a technical question for Dr. Schou or other IATAC SMEs, please contact iatac@dtic.mil. The IATAC staff will assist you in reaching the SME best suited to helping you solve your challenge at hand. If you have any questions about the SME program or are interested in joining the SME database and providing technical support to others in your domains of expertise, please contact iatac@dtic.mil, and the URL for the SME application will be sent to you. ■

References

1. More information about (ISC)2 can be found at *http://www.isc2.org*
2. More information about NIATEC can be found at *http://niatec.info*
3. More information about the IAP can be found at *http://security.isu.edu*
4. More information about CISSE can be found at *http://cisse.info*

A Decade of Air Force and Academic Collaboration Toward Assuring Information

by Kevin Kwiat, Shambhu Upadhyaya, and Amber Helton

Introduction

At first, Dr. Kevin Kwiat of the Air Force Research Laboratory (AFRL) in Rome, NY, and Dr. Shambhu Upadhyaya of the University at Buffalo (UB), NY, independently pursued research in fault tolerance. Dr. Kwiat was applying field-programmable gate array (FPGA) technology to create a hardware-accelerator [1] that shortens the gap between when a fault is encountered and the continuation of error-free computation. Dr. Upadhyaya was performing testing and fault diagnosis, coupled with schemes for the sparing of modules to recover from failure-inducing faults. [2, 3]

Then in 1997, the two men came together by chance when they presented their research at the same technical symposium. At that time, information assurance (IA) had come to the forefront; the intensity and severity of information attacks were driving researchers to consider new ways of defending information systems. To Drs. Upadhyaya and Kwiat, defense might come in the form of transforming fault tolerance techniques. No longer could faults be considered random; rather, faults that emerged from the damage that an attacker inflicted would be not only non-random but also made to occur at critical times and places so that they might subsequently undermine previous applications of fault tolerance. Techniques for tolerating these attacker-induced faults could not simply be adopted from the existing field of fault tolerance; instead, they had to be adapted.

Exploring the adaptation of fault tolerance for IA became the motivation behind Dr. Upadhyaya's and Dr. Kwiat's collaboration, and it became formal when Dr. Upadhyaya became the first National Research Council (NRC) Summer Faculty Fellow to join AFRL's Information Directorate (AFRL/RI). With Dr. Kwiat as his mentor, and with support from the Air Force Office of Scientific Research (AFOSR) to underwrite Dr. Upadhyaya's summer research, the two began addressing what was driving the need to adapt, not adopt, fault tolerance for IA—the attacker.

A Simulation Platform for Intrusion Detection in Distributed Systems

Attackers who successfully intrude through pervious computer defenses have a capability to retrieve data and confidential resources. This capability can render traditional fault tolerance ineffective; therefore, the capability must be prevented. Even though an intrusion detection system (IDS) may identify malicious intents, it does not fully prevent intruders from compromising data on a system. [4]

Drs. Upadhyaya and Kwiat determined that expediting intrusion detection was paramount: lessening the time attackers go undetected lessens their ability to induce faults. Detection time could be dramatically abbreviated when the user's intent was known a priori; therefore, Drs. Upadhyaya and Kwiat devised a technique for encapsulating the user's explicitly expressed intent before enabling the user's session on a computer. [5] On the host computer, an auxiliary process would query a new user for a session scope from which an assertable strategy, called the Sprint Plan, would be generated. The Sprint Plan consisted of carefully derived, session-specific, assertions for real-time attack monitoring. Experiments demonstrated that encapsulating a user's intent for session-specific assertion checking provided low performance overhead, timely detection, and improved coverage—all with acceptable false positives. [6]

Specification and Verification of a Secure Distributed Voting Protocol

As their work on intrusion detection progressed and yielded encouraging results, Dr. Kwiat founded the Assured Communications Research Center (ACRC) in 2000. The ACRC is an in-house research program aimed at adapting fault tolerance for IA. Joining the ACRC was Air Force 1st Lt Benjamin Hardekopf. Along with Drs. Kwiat and Upadhyaya, he concluded that the IDS, although improved, could never be perfect; before an intrusion is detected, the computer system might have damage inflicted on it. Applicable fault tolerance techniques called for replication to allow correct operation, even in the presence of some faulty replicas, and voting among the

replicas resolves the redundant output from each replica to provide a single, fault-free system output.

Once again, the pessimistic assumption that an attacker is able to non-randomly insert faults into a system resulted in taking a voting algorithm suitable for fault tolerance and transforming it for IA settings. The ACRC researchers' solution, called the Timed Buffer Distributed Voting Algorithm (TBDVA), would be warranted for critical applications requiring assurance against accidental and intentional faults. Using Temporal Logic of Actions (TLA) and TLA+, Lt Hardekopf formally proved that TBDVA met its IA specification. Much of Lt Hardekopf's in-house work on TBDVA became material for his thesis, for which he received a master of science in computer science at the State University of New York at Utica/Rome. The ACRC work on TBDVA resulted in a US patent and an in-house technical report [7] that covered several conference and symposia papers (*e.g.*, [8, 9]) dealing with the ongoing evolution of TBDVA.

> Attackers who successfully intrude through pervious computer defenses have a capability to retrieve data and confidential resources. This capability can render traditional fault tolerance ineffective; therefore, the capability must be prevented.

Mobile Computing—Implementing Communications Technologies

Occasionally, the benefits of research are not direct results; they are insights. For instance, in 2002, Drs. Kwiat and Upadhyaya became co-editors for Mobile Computing, [10] a book addressing the many business and technical issues confronting the emergence of pervasive computing. The insights gained from their collaborative research enabled them to shape Mobile Computing as a macrocosm of the ACRC: that key adaptations of current developments could propel the state of the art to its next intended destination. They determined that reaching the hallmarks of pervasive computing—to compute every time, everywhere—could be achieved through the directed research of the book chapters' authors whose efforts contended with the limitations of technology and policy at the beginning of the 21st century.

Recognition for IA Contribution

The ACRC grew with the addition of an adjunct member. Mr. Ramkumar Chinchani, a UB student, conducted his doctoral research using Air Force Office of Scientific Research (AFOSR) support aimed at enhancing the ACRC. He expanded on the notion of encapsulating a user's intent in their user-level IDS; earlier versions depended on a user's explicit expression of their intent, but Mr. Chinchani created a capability for capturing a user's intent implicitly. Users' actions were closely monitored, and Mr. Chinchani's system would recognize when users performed tasks that became routine.

With this knowledge, a Sprint Plan was generated that did not require users to foretell the intent of their computer usage. In 2002, Drs. Upadhyaya and Kwiat and Mr. Chinchani chose, as a conference venue, the Military Communications Conference (MILCOM) [11] to document their latest developments of their intrusion detection work. Dr. Kwiat presented the group's paper, and the presentation must have been propitious because the research was cited in Scientific American. [12] Shortly after, the popular press [13] provided further coverage with a story about the endeavors of the three researchers. The Associated Press story focused on society's growing concerns about information system security.

In his interview for the story, Dr. Upadhyaya explained that user-level intrusion detection by encapsulation of user's intent was designed to surpass other computer-security products that featured user-profiling techniques by citing that other products were generally 60 to 80 percent reliable, whereas the encapsulation method demonstrated up to 94 percent reliable detections while simultaneously keeping false alarms to an acceptable level. Although demonstrably effective, Dr. Upadhaya noted that user-level intrusion detection by encapsulation of user's intent would be only one of thousands of tools in a computer-security arena requiring multilayered defenses. [13]

Detection of Attacks in User Space

In Dr. Upadhyaya's interview, he also expressed the opinion that society's malaise over computer security was justified by citing how more experienced hackers were recruiting young teenagers with computer skills to join in on their malevolent endeavors. [14] Alarmingly, the skill level of these new recruits was not paramount; instead, the experienced hackers were creating toolkits whereby even a nascent attacker could inflict damage on a targeted information system. In response, the ACRC team took a more pessimistic, inward view; in 2003, they launched a new year of intrusion detection research introducing a revised approach to their intrusion detection scheme.

Previously, they demonstrated that the theory of encapsulating a user's intent for user-level intrusion detection would work; however, they reinspected the implementation of that theory. Speed and efficiency had been compelling reasons to place the intrusion detection software in the same memory space on the computer as the user's processes. In retrospect, such a placement made the intrusion detection software vulnerable to attacks aimed at disabling an information system's protection so that the attacker would then have free reign over the system.

At the 2003 Institute of Electrical and Electronics Engineers (IEEE) International Information Assurance Workshop in Darmstadt, Germany, the team presented a paper, A Tamper-Resistant Framework for Unambiguous Detection of Attacks in User Space Using Process Monitors. [15] This paper described a mechanism that eventually became known as the Progressive Attack Reactors and Nexus of Intrusion Detection (PARANOID). In the PARANOID framework, the IDS is monitored by a lightweight process in operating system (OS) kernel space that is monitored in turn by a similar process, which is then monitored by another lightweight process, and so on until a circular chain of mutually inspecting monitors is formed. The framework protects the protector; if the IDS or any of the monitors is suddenly disabled, then a surviving monitor raises an alarm. Thus, penetrating PARANOID and escaping detection requires an attacker to disable all monitors simultaneously—a more difficult feat than simply disabling only the intrusion protection software. One insight that was gained from implementing PARANOID was that not all OSs at that time provided the support needed for performing asynchronous event monitoring.

Secure Knowledge Management

In the case of PARANOID, successful implementation of the prototype required matching it to an OS with adequate support features. In a wider sense, this indicated that prescriptions for success in transitioning IA concepts from theory to implementation to practice would require a broader understanding among all stakeholders. Drs. Upadhyaya and Kwiat considered how to translate this experience into action; yet, they realized that disseminating knowledge (to enable understanding) might itself require applying IA. In 2004, AFRL/RI co-sponsored, through the ACRC, the Workshop on Secure Knowledge Management held at UB. The workshop aimed to raise awareness of academics and practitioners in secure knowledge management. Knowledge management systems (KMS) promote information sharing to increase productivity; however, the US Government and other organizations have concerns involving KMS. These concerns are based on the preponderance of web access and intranets as well as the increasing importance of securing corporate knowledge, especially as companies continue to grant access to numerous individuals.

Before the workshop, the National Security Agency (NSA) had already selected UB as a Center of Academic Excellence in Information Assurance Education. Dr. Upadhyaya is the UB Center's director. Under the leadership of UB Center Director Dr. Upadhyaya, the center has brought more than a million dollars in external funding in support of IA activities, including student scholarships and laboratory research and development. In 2007, Dr. Kwiat became a member of UB Center's advisory board.

User-Level Intrusion Detection

In 2005, the intrusion detection work reached another milestone when Mr. Chinchani defended his doctoral dissertation, A Job-Centric Approach to User-Level Intrusion Detection, [16] with Dr. Upadhyaya serving as his advisor and Dr. Kwiat as a member of the defense committee. That same year, the three co-authored a book chapter. [17] Dr. Chinchani's dissertation, in addition to documenting issues concerning user-level intrusion detection, included several advancements. One advancement was a proposed higher order representation of a user profile in which the system documents steps that the user takes to properly carry out commands. This advancement would ensure user involvement in the security process to further lower rates of false positives.

Graphical User Interface Based Systems

In 2006, the user-level intrusion detection work took on a different dimension. Drs. Upadhaya and Kwiat were joined by two fellow student researchers at UB: Mr. Ashish Garg and Ms. Ragini Rahalkar. They expanded the user-level intrusion detection scheme beyond the monitoring of a user's commands under the governance of a Sprint Plan. By considering how a user manipulates a computer's graphical user interface (GUI), their system could discern between a genuine user or a masquerader. [18] The team introduced a new framework that created an individual feature set for a user's behavior on GUI systems. Team members collected real user behavior data from live systems and removed limitations to create feature vectors. These vectors contained user information such as mouse angles, speed, and number of clicks during a user session. Their prototype demonstrated that user behavior features based on mouse activity on a GUI system uniquely identified users. This effort provided better masquerade detection capabilities. [18]

A decade of collaboration is now complete. Collaboration that served as a seedbed for new projects in the Air Force and academia—AFRL/RI's ACRC and the UB's Center of Excellence in IA Education—continues

Loss Inference in Networking

On obvious lesson from the user-level intrusion detection work was that as more information is gathered about a user (*e.g.,* user's intent and feature vectors of GUI behavior), then the more likely that IA would be met. Drs. Kwiat and Upadhyaya considered what less information meant in the context of IA. Quality of service (QoS) quantifies data usability and availability with respect to the end user. QoS loss in networks can be attributed to random effects (*e.g.,* network congestion) or attack (*e.g.,* denial of service attack [DoS]). In some situations, the end user is capable of automatically inferring the status of the QoS; however, in most scenarios, an accurate determination cannot be made on the source of a QoS disruption. Such special situations make the identification of the root cause of a QoS loss even more paramount because incorrect user action could worsen the problem. An application viewed by the user as nonresponsive may be rebooted, causing a self-DoS, whereas the actual problem stemmed from prolonged network latency.

The benefits of appropriate feedback are obvious: the end user is in a position to not only accurately trace the loss of QoS to its root but also initiate appropriate action instead of the more often observed behavior of implicitly assuming that the local application is probably at fault. Generally, a fault is an event in which a system operates contrary to its specification, although this may be invisible to system users. [19] The challenge was to locate the fault—that is, infer the cause for information loss…or simply, make the invisible—visible. Teamed with UB doctoral student Mr. Vidyaraman Sankaranarayanan, in 2007 they devised a game-theoretic scheme that makes the inference; it can distinguish between adversarial network exploitation and benign network loss. [20]

Conclusion

A decade of collaboration is now complete. Collaboration that served as a seedbed for new projects in the Air Force and academia—AFRL/RI's ACRC and the UB's Center of Excellence in IA Education—continues. The longevity of the collaboration is an indication of the merits of the objective: to create computer systems that operate correctly, even though parts of these systems are malfunctioning, regardless of the malfunction's source. ■

References

1. Kevin Kwiat. Dynamically Reconfigurable FPGA-Based Multiprocessing and Fault Tolerance. Doctoral Dissertation. Graduate School of Syracuse University, 1996, Syracuse, NY.
2. Robert Spina, Shambhu Upadhyaya, "Linear Circuit Fault Diagnosis Using Neuromorphic Analyzers," IEEE Transactions on Circuits and Systems-II, March 2007, Vol. 44, No. 3, pp.188–196.
3. Yung-Yuan Chen, Shambhu Upadhyaya, Ching-Hwa Cheng, "A Comprehensive Reconfiguration Scheme for Fault-Tolerant VLSI/WSI Array Processors," IEEE Transactions on Computers, December 1997, Vol. 4, No. 12, pp 1363–1370.
4. "Intrusion Detection FAQ," Sans Institute, Version 1.80, 9 July 2007, The Sans Institute of Technology, 21 June 2007. *http://www.sans.org/resources/idfaq*
5. Kevin Kwiat, Shambhu Upadhyaya, "A Distributed Concurrent Intrusion Detection Scheme Based on Assertions," 1999 SCS Symposium on Performance Evaluation of Computer and Telecommunication Systems, July 1999, Chicago, IL, pp. 369–376.
6. Kevin Kwiat, Shambhu Upadhyaya, "A Comprehensive Simulation Platform for Intrusion Detection in Distributed Systems," The Proceedings of the 2000 Summer Computer Simulation Conference, Simulation Councils, Inc., 2000, Vancouver, British Columbia, pp. 586–591.
7. Benjamin Hardekopf, Kevin Kwiat, Distributed Voting for Security and Fault-Tolerance, May 2001 In-House Report: Air Force Research Laboratory, Information Directorate, Rome, NY: AFRL-IF-RS-TR-2001-53.
8. Benjamin Hardekopf, Kevin Kwiat, Shambhu Upadhyaya, "Specification and Verification of a Secure Distributed Voting Protocol," 2001 International Symposium on Performance Evaluation of Computer and Telecommunication Systems, Simulation Councils, Inc., 2001, Orlando, FL, pp. 535–545.
9. Benjamin Hardekopf, Kevin Kwiat, Shambhu Upadhyaya, "Secure and Fault-Tolerant Voting in Distributed Systems," 2001 IEEE Aerospace Conference, Big Sky, Montana, March 2001.
10. Shambhu Upadhyaya, Kevin Kwiat, Abhijit Chaudhury, Mark Weiser (eds.), *Mobile Computing: Implementing Pervasive Information and Communication Technologies,* Kluwer Academic Publishers Book Series on Interfaces in Operations Research and Computer Science, June 2002.

11. Ramkumar Chinchani, Shambhu Upadhyaya, Kevin Kwiat, "Towards the Scalable Implementation of an Anomaly Detection System," Proceedings of the Military Communications Conference (MILCOM) 2002, Anaheim, CA, USA 2002.
12. Charles Choi, "Computer Security: Keyboard Cops," Scientific American, 16 November 2002, Scientific American.com, 21 June 2007. *http://www.cse.buffalo.edu/~rc27/projects/DRUID/press/scientificamdec02.pdf*
13. Ben Dobbin. "New Software Aims to Snare Computer Intruders in Real Time," The Associated Press Bulletin, 23 January 2003, The Associated Press, 10 July 2007. *http://www.team-ninja.com/vbulletin/archive/index.php/t-19610.html*
14. John Lasker, "Hackers Use Computer Skills to Promote Politically MotivatedMischief, Mayhem," Knight Rider Tribune Business News, 14 May 2002, Washington, 10 July 2007. *http://www.accessmylibrary.com/coms2/summary_0286-8624483_ITM*
15. Ramkumar Chinchani, Shambhu Upadhyaya, Kevin Kwiat, "A Tamper-Resistant Framework for Unambiguous Detection of Attacks in User Space Using Process Monitors," IEEE International Information Assurance Workshop, 2003, Darmstadt, Germany, pp. 25–33.
16. Ramkumar Chinchani, "A Job-Centric Approach to User-Level Intrusion Detection," Doctoral Dissertation, Graduate School of the State University of New York at Buffalo, 2005, Buffalo, NY.
17. Shambhu Upadhyaya, Ramkumar Chinchani, Kiran Mantha, Kevin Kwiat, "Encapsulation of User's Intent: A New Proactive Intrusion Assessment Paradigm," (book chapter) in Managing Cyber Threats: Issues, Approaches and Challenges, Kluwer Academic Publishers, 2005.
18. Ashish Garg, Ragini Rahalkar, Kevin Kwiat, Shambhu Upadhyaya, "Profiling Users in GUI Based Systems for Masquerade Detection," Seventh IEEE SMC Information Assurance Workshop, CD-ROM, 1st ed. 21–23 June 2006, West Point, NY.
19. Jonar C. Nader, Illustrated Dictionary of Computing, Prentice Hall Publishers, 1992.
20. Vidyaraman Sankaranarayanan, Kevin Kwiat, Shambhu Upadhyaya, "QoS-LI: QoS LossInference in Disadvantaged Networks," IEEE Computer Society 21st International Conference on Advanced Information Networking and Applications Workshops/Symposia, 2007, Los Alamitos, CA, pp. 524–529.

About the Authors

Dr. Kevin A. Kwiat | is a computer engineer and program manager with the Air Force Research Laboratory's Information Directorate in Rome, NY. His research focuses on adapting concepts from the fault tolerant computing domain to cyber defense. He holds a BS in Computer Science, BA in Mathematics, Masters in Computer Engineering, and PhD in Computer Engineering, all from Syracuse University. Dr. Kwiat teaches courses at Syracuse University as part of their MS in Computer Engineering – Assurance Tracks, and holds three US patents.

Dr. Shambhu J. Upadhyaya | is an associate professor of Computer Science and Engineering at the University at Buffalo. His research interests are in information assurance, fault tolerant computing, and very large-scale integration (VLSI) testing. He has a BE and ME in electrical engineering from the Indian Institute of Science, Bangalore, India. He holds a PhD in Electrical and Computer Engineering from the University of Newcastle, Australia. He is also a visiting research faculty member at the Air Force Research Laboratory in Rome, NY, and holds a US patent.

Ms. Amber N. Helton | is an electrical and computer engineering student at the University of Louisville Speed School of Engineering in Kentucky. She is a Reserve Officer Training Corps (ROTC) summer intern for the Air Force Research Laboratory's Assured Computing Research Center in Rome, NY. She also is a member of the Air Force Advanced Course in Engineering (ACE) Cyber Security Boot Camp Class of 2007. Her research with the Air Force includes cyber security policies, digital forensics, network architecture, malicious code, and cyber warfare.

Letter to the Editor

Q ***Recommend updating the IATAC IA Digest to include the next generation of the IASE Web site—the DoD IA Portal on DKO.***

A One of our readers, Mr. Walter Kelley, Defense Information Systems Agency (DISA), made the excellent recommendation above. After receiving this comment, we took immediate action to update the IA Digest, which now reflects the current Department of Defense (DoD) Information Assurance (IA) Portal. On 30 April 2007, the IA Portal began initial operating on Defense Knowledge Online (DKO). The IA Portal is indeed the "next generation" of the Information Assurance Support Environment (IASE) Web site. The DoD recognized the need for a more enhanced way to service the entire IA community. The new portal enables the community to collaborate and share IA-related information and knowledge *via* multiple avenues, including email, chat, Instant Message (IM), collaborative tools, forums, and documents.

To use the IA Portal, you must have a DoD common access card (CAC) and be registered for a DKO account. To register, simply visit the Army Knowledge Online/Defense Knowledge Online (AKO/DKO) Web site *https://www.us.army.mil* and follow DKO registration steps. Once registered, you may use the myriad services that the AKO/DKO offers, including the IA Portal. ■

FREE Products

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 online: *http://www.dtic.mil/dtic/registration*. The *IAnewsletter* is UNLIMITED DISTRIBUTION and may be requested directly from IATAC.

Name ______________________________ DTIC User Code ______________________________

Organization ______________________________ Ofc. Symbol ______________________________

Address ______________________________ Phone ______________________________

______________________________ Email ______________________________

______________________________ Fax ______________________________

Please check one: □ USA □ USMC □ USN □ USAF □ DoD
□ Industry □ Academia □ Government □ 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) □ Configuration Management □ Defense in Depth (soft copy only)
□ Data Mining (soft copy only) □ IA Metrics (soft copy only) □ Network Centric Warfare (soft copy only)
□ Wireless Wide Area Network (WWAN) Security □ Exploring Biotechnology (soft copy only)
□ Computer Forensics* (soft copy only. DTIC user code MUST be supplied before these reports will be shipped)

State-of-the-Art Reports (SOARs)

□ Data Embedding for IA (soft copy only) □ IO/IA Visualization Technologies (soft copy only)
□ Modeling & Simulation for IA (soft copy only) □ Malicious Code (soft copy only)
□ Software Security Assurance □ A Comprehensive Review of Common Needs and Capability Gaps

UNLIMITED DISTRIBUTION

IAnewsletters Hardcopies are available to order. The list below represents current stock.
Softcopy back issues are available for download at *http://iac.dtic.mil/iatac/IA_newsletter.html*

Volumes 4		□ No. 2	□ No. 3	□ No. 4
Volumes 5	□ No. 1	□ No. 2	□ No. 3	□ No. 4
Volumes 6	□ No. 1	□ No. 2	□ No. 3	□ No. 4
Volumes 7	□ No. 1	□ No. 2	□ No. 3	□ No. 4
Volumes 8	□ No. 1	□ No. 2	□ No. 3	□ No. 4
Volumes 9	□ No. 1	□ No. 2	□ No. 3	□ No. 4
Volumes 10	□ No. 1	□ No. 2	□ No. 3	

Fax completed form to IATAC at 703/984-0773

Calendar

November

CSI 34th Annual Computer Security Conference
5-7 November
Washington, DC
http://www.csi34th.com

Global MilSatCom 2007
5-7 November
London, United Kingdom
http://www.smi-online.co.uk/events/overview.asp?is=1&ref=263

Air Intelligence Agency Internal Information Assurance & IT Conference
5-7 November
San Antonio, TX
https://www.technologyforums.com/7AI

11th Annual Small Business Conference
7-8 November
Tysons Corner, VA
http://www.ndia.org/Template.cfm?Section=8430&Template=/ContentManagement/ContentDisplay.cfm&ContentID=16926

TechNet North 2007 C4ISR
14-15 November
Boston, MA
http://www.tnnorth.org

IEEE Global Communications Conference 2007
26-30 November
Washington, DC
http://www.ieee-globecom.org/2007/index.html

December

Counterintelligence Symposium
4 December
Sunnyvale, CA
http://afcea.org/events/counterintel/welcome.asp

NextGens Technologies
5-6 December
Santa Monica, CA
http://www.ttivanguard.com/conference/2007/santamonica.html

The Summit on Virtualization
7 December
New York, NY
http://www.misti.com/default.asp?page=65&Return=70&ProductID=7508

Open Technology
11-12 December
Vienna, VA
http://www.afei.org/brochure/8a03/index.cfm

January

2008 DoD Cyber Crime Conference
13-14 January – Pre-Conference Training
14-15 January – Exposition
14-18 January – Conference
St. Louis, MO
http://www.dodcybercrime.com

IATAC

Information Assurance Technology Analysis Center
13200 Woodland Park Road, Suite 6031
Herndon, VA 20171

To change, add, or delete your mailing or email address (soft copy receipt), please contact us at the address above or call us at: 703/984-0775, fax us at: 703/984-0773 , or send us a message at: iatac@dtic.mil