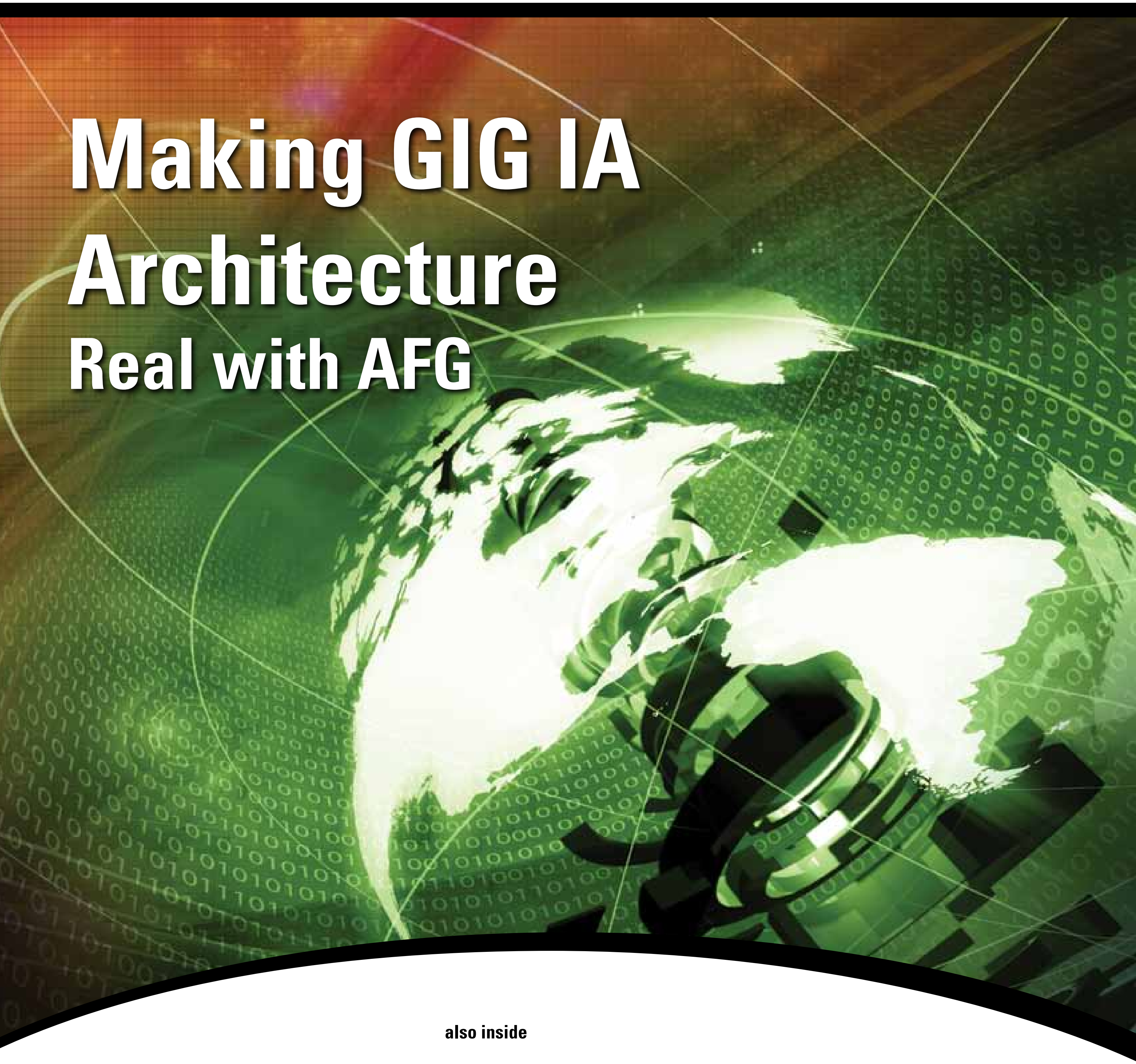
12/1

Volume 12 Number 1 • **Spring 2009**

IAnewsletter

The Newsletter for Information Assurance Technology Professionals



Making GIG IA Architecture Real with AFG

also inside

IATAC

contents

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 &
Creative Director: Christina P. McNemar
Art Director: Don Rowe
Copy Editors: Louis Price
Linda Billard
Kali Wilson
Designers: Ricardo Real
Dustin Hurt
Don Rowe
Editorial Board: Dr. Ronald Ritchey
Angela Orebaugh
Dennis Storey
Kristin Evans
Gene Tyler

***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
Fall 2009 March 27th, 2009

Cover design: Ricardo Real
Newsletter design: Donald Rowe

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

in every issue

IATAC Chat

Gene Tyler, IATAC Director

The IA and knowledge communities are active and this edition of the *IAnewsletter* is full of interesting and valuable information starting with a short article about IATAC's latest SOAR—*The Insider Threat to Information Systems: A State-of-the-Art Report (SOAR)*. The SOAR was written by IATAC Subject Matter Experts (SMEs) after extensive coordination with government, industry, and academic experts in this field. It provides a comprehensive look at the most significant of today's efforts in government, industry, and academia to detect and combat the wide variety of insider threats to operational information systems and to the information technology supply chain. Because this Report is unclassified but contains FOUO information, distribution is limited to US Government and authorized contractors. Please register with the Defense Technical Information Center (DTIC), the Total Electronic Migration System (TEMS), or contact IATAC to obtain a copy. This report, as with all of our other SOARs, is free and comes in book form (until supplies are exhausted) or you can obtain a copy of an electronic version—many find this media to be best for their research needs. You can always go to the IATAC website *http://iac.dtic.mil/iatac/* to obtain copies of SOARs and other products.

IATAC is moving forward with its portion of a Government sponsored wiki targeted to the research and development/science and technology (R&D/S&T) communities—DoDTechipedia. This does not mean it is limited to the R&D/S&T communities—my guess is if you are interested in IA you can find areas of interest. DoDTechipedia is not limited to just IA—you can find information from Armor Technologies, Electro-Optical Infrared Sensors, Microelectronics to Wireless Technologies—I think you will find something that interests you. This project is unique and exciting in that it is an unofficial vehicle for social collaboration and each section has subject matter experts performing the wiki-like gardening. IATAC will garden and care for the IA subject areas and will post important conference and symposium information too. The DoDTechipedia website, *https://www.dodtechipedia.mil/dodwiki*, is a protected website so if you need assistance email *reghelp@dtic.mil* or telephone DTIC's Registration Team at 800/225-3842, menu selection 2, option 1 or 703/767-8273 or DSN 427-8273. Of course IATAC can help with IA technical/gardening questions – contact Mr. Rogelio Raymond (703/984-0072, *iatac@dtic.mil*).

As usual you will find a host of other useful information in this edition. The article from COL Surdu, Chief of Staff Army's Research, Development, and Engineering Command and LTC Conti, Assistant Professor US Military Academy (West Point)—*Army, Navy, Air Force, and Cyber—Is it Time for a Cyberwarfare Branch of the Military?* is thought provoking and provides an interesting question for our netcentric forces that are reliant on a Global Information Grid not bounded by traditional Service boundaries. And, if you are interested in an IA perspective from the industry, business, and academic communities read the *Secure Content Automation Protocol (SCAP) for the Enterprise Ask The Expert* piece by Allan Carey of the Institute for Applied Network Security (IANS) when he talks about what SCAP is. That said, I think you will find all articles provide some interesting insight.

As always, I look forward to your thoughts and comments—lets us know what you think by email at *iatac@dtic.mil* or call us at 703/984-0775. We welcome you comments and suggestions.

See you in February at the Information Assurance Symposium in Dallas!!! ■

Gene Tyler

Making GIG IA Architecture Real with AFG

by Keith D. Willet and Stephen G. York

The intent of Alignment Framework for the GIG (AFG) is to convey GIG IA Architecture guidance in context of other existing IA guidance. Existing IA guidance includes DoD Instruction 8500.2 *Information Assurance Implementation* and Director of Central Intelligence Directive (DCID) 6/3 [1] *Protecting Sensitive Compartmented Information within Information Systems,* among others.

To prepare for the future protection of national interests, the United States Department of Defense (DoD) is moving toward operation within a Net-Centric (NC) operating environment. The Information Assurance Directorate (IAD) of the National Security Agency (NSA) is defining and generating guidance to achieve assured Net-Centricity (assured NC). Achieving the complex and long term objective of assured NC requires an architecture promoting many disparate operations and acquisition programs to moving toward the common goals of achieving assured access, collaboration, and information sharing.

Acquisition programs face the challenge of interpreting the architectural vision while maintaining a primary focus on system development, both within budget and according to schedule. To aid the acquisition Program Managers in this challenge, the authors of GIG IA Architecture v1.1 (the NSA IAD *Enterprise IA Systems Engineering Services Office*) have taken steps toward simplifying the delivery mechanism of GIG IA architectural guidance through the Alignment Framework for GIG IA Architecture (AFG).

AFG provides templates, guides, and a methodology to make GIG IA Architecture v1.1 understandable and actionable at the acquisition program level. AFG is useful to acquisition program Information System Security Engineers (ISSEs), other IA professionals, and Program Managers desiring to integrate GIG IA guidance in their solutions. AFG helps make GIG IA architecture real at the acquisition program level.

A Response to Community Challenges

IAD published the GIG IA Architecture v1.1 on 16 November 2006. With respect to GIG IA, DoD challenges broadly apply to the Intelligence Community (IC) and the United States Government (USG). These challenges include—

- Achieving an understanding of assured GIG concepts
- Determining how to incorporate GIG IA Architecture into the Net Ready Key Performance Parameter (NR KPP) documentation required by Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01
- Learning how to incorporate GIG IA Architecture alignment into Clinger-Cohen Act (CCA) compliance
- Knowing how to overcome these challenges when direct, hands-on support from NSA is not available.

IAD challenges include the following—

- The need to simplify the assured GIG concepts
- The need to distill the GIG IA Architecture into understandable and actionable terms

- The need to align GIG IA guidance with existing security controls recognized across the USG
- The need to extend the reach of IAD expertise into NSA's client space without direct NSA contact.

The answer to these challenges is the AFG. The AFG provides tools and a methodology to plan, assess, track, and report on alignment with GIG IA Architecture guidance. The intent of AFG is to convey GIG IA Architecture guidance in context of other existing IA guidance. Existing IA guidance includes DoD Instruction 8500.2 *Information Assurance Implementation* and Director of Central Intelligence Directive (DCID) 6/3 [1] *Protecting Sensitive Compartmented Information within Information Systems*, among others. Future security controls for DoD and the IC will center on the *Committee for National Security Systems Instruction (CNSSI) 1253 Security Controls Catalog (SCC).* [2] GIG IA Architecture is focused on net-centric, enterprise IA guidance, while other IA guidance focuses more on the use of security controls. Both guidance sources are important to establish and maintain an effective GIG IA posture.

GIG IA and the Defense-Wide IA Program (DIAP)

The Defense -Wide IA Program (DIAP), in its Acquisitions and Technology Oversight role, assists programs during the acquisition process. As articulated in its mission statement, DIAP's responsibilities include the following task—

> *To ensure the DoD's vital information resources are secured and protected by unifying/integrating IA activities to achieve secure Net-Centric GIG operations enablement and information superiority by applying a Defense-in-Depth methodology which integrates the capabilities of people, operations, and technology to establish a multi-layer, multi-dimension protection.* [3]

DIAP provides oversight to ensure programs comply with the CCA. Its position is that CCA requires all acquisitions of mission-critical/mission-essential information technology (IT) to have "… an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards." A DIAP goal is to leverage AFG to provide acquisition programs with an objective method to plan and assess their alignment with the GIG IA Architecture v1.1. Acquisition programs will provide alignment details as

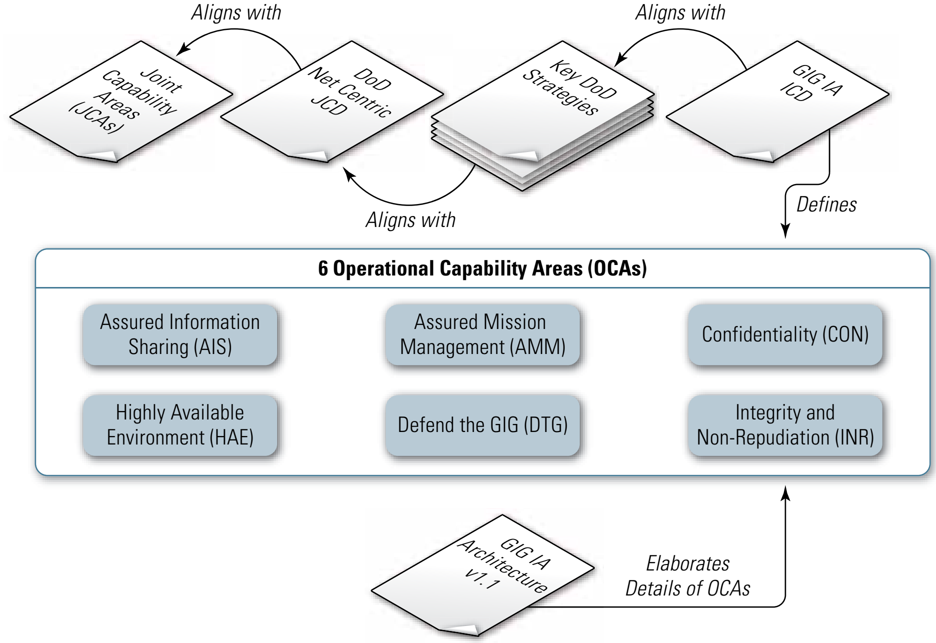

Aligns with
Aligns with
Joint Capability Areas (JCAs)
DoD Net Centric JCD
Key DoD Strategies
GIG IA ICD
Aligns with
Defines
6 Operational Capability Areas (OCAs)
Assured Information Sharing (AIS)
Assured Mission Management (AMM)
Confidentiality (CON)
Highly Available Environment (HAE)
Defend the GIG (DTG)
Integrity and Non-Repudiation (INR)
GIG IA Architecture v1.1
Elaborates Details of OCAs

Figure 1 JCA—GIG IA Architecture Relationship

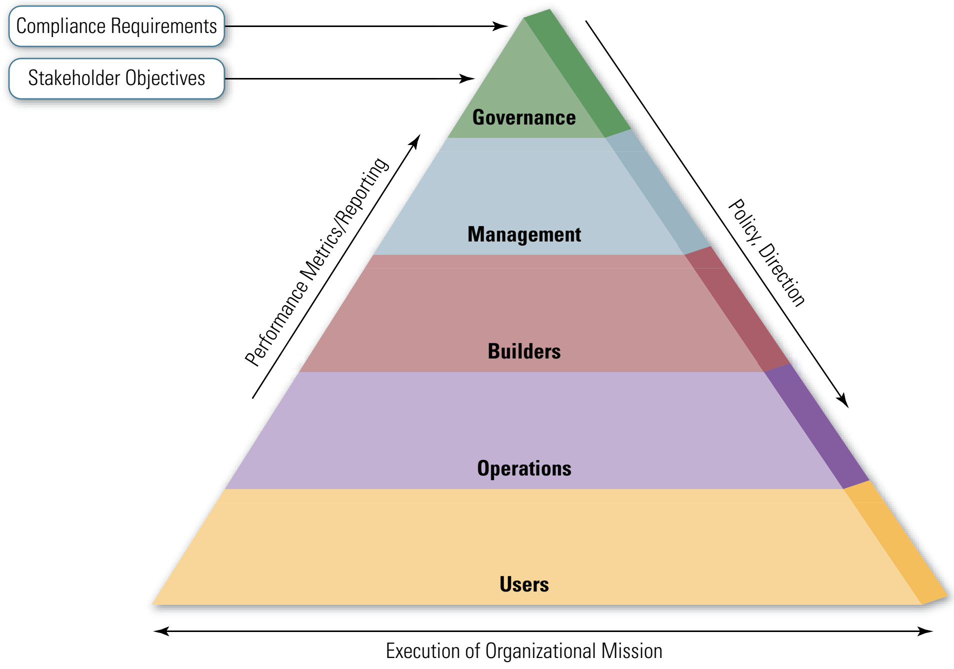


Figure 2 Organizational Role Views of IA

part of a Component Chief Information Officer (CIO) attestation to DIAP confirming CCA compliance.

GIG IA and Mission Capabilities

Joint Capability Areas (JCAs) establish the lexicon of what DoD will do for the Federal Community and the US citizen. JCAs articulate capabilities that appear in Joint Capabilities Integrated Development System (JCIDS) concepts and identify JCIDS artifacts that flow into the acquisition process. The GIG is an instance of the Net-Centric philosophy; GIG IA, or an assured GIG, is an instance of assured Net-Centricity. GIG IA started as a concept stated in the GIG IA Initial Capability Document (ICD) in support of key DoD strategies, (*e.g.,* DoD Net-Centric Data Strategy) and DoD Net-Centric Joint Capability Document (JCD). The GIG IA ICD presents six Operational Capability Areas (OCAs) (Figure 1). The GIG IA Architecture v1.1 elaborates the first steps toward achieving an assured GIG in terms of the OCAs.

The AFG relates GIG IA Architecture v1.1 guidance with associated systems engineering guidance and aligns both of these with security controls familiar to the community.

IA in the Enterprise

Like a diamond, the enterprise is multifaceted with many dimensions across people, processes, technologies, environments, and services. IA does not define the value of enterprise; IA does help to preserve the value of the enterprise.

IA is one of many enterprise facets; moreover, there are many facets within IA—each offering a different perspective. The various facets of IA do not look at different things, but rather look at the same thing with different interests and objectives. IA facet views include—

- ▶ Joint Capability Areas
- ▶ Joint Capabilities Integrated Development System
- ▶ Acquisition Process
- ▶ Portfolio Management (PfM)
- ▶ Enterprise Architecture (EA)
- ▶ Systems Engineering (SE)
- ▶ Operational Capability Area (OCA)
- ▶ Operational Capability (OC)
- ▶ IA System Function.

The JCAs help DoD describe the various mission facets that the United States requires for National Security—IA ensures that those DoD National Security related missions are protected from attacks on and failures of the information technology supporting those missions. IA is both an official mandate as well as good business practice. IA, in its entirety, does not belong to anyone; establishing and maintaining effective IA is a responsibility shared by all. According to their role, some organizations have primary responsibility for certain aspects of IA. Organizational role views of IA (Figure 2) include governance, management, builders, operations, and users. The GIG IA Portfolio Management (GIAP) prioritizes and manages enterprise investments in IA. The NSA Information Assurance Directorate has primary responsibility of generating guidance to achieve an assured GIG.

A multi-dimensional view of IA is necessary to accommodate the breadth and depth of IA planning, acquisition, implementation, and operation.

AFG Overview

The AFG has a structure specifically designed to convey GIG IA Architecture guidance in terms of security controls familiar to the community. AFG is both a *methodology* for use by Acquisition programs and a *content manager* aligning and integrating GIG IA Architecture guidance with existing and future IA guidance for the DoD, the IC, and the USG.

AFG Structure

The structure of AFG is based on the Committee on National Security Systems Instruction 1253 (CNSSI 1253) Security Controls Catalog (SCC). CNSSI 1253 defines a set of security controls as a basis for a Certification and Accreditation (C&A) process applicable to national security systems across the USG. The CNSSI 1253 is based on National Institute of Standards and Technology (NIST) Special Publication 800-53, plus guidance from DoDI 8500.2 and DCID 6/3; that is, CNSSI 1253 is a superset of this other guidance.

Moreover, there is increased effort to synchronize CNSS work with NIST work to provide a very similar look and feel to security controls across the DoD, the IC, and the USG. The AFG Framework—the structure of AFG—aligns with CNSSI 1253 to present GIG IA Architecture guidance in terms of security controls familiar to the community. All traceability from AFG to JCAs and to configuration guidance (*e.g.* Federal Desktop Core Configuration (FDCC) occurs via the AFG Framework; any content placed within the AFG Framework then inherits these traces.

AFG Content

The AFG Content is the GIG IA Architecture v1.1 guidance. Additionally, there is explicit traceability from AFG to DoDI 8500.2 and DCID 6/3. This traceability gives GIG IA Architecture an agile relationship to evolving IT security controls, from the current set of security controls (*e.g.,* DoDI 8500.2 and DCID 6/3) to future set(s) of security controls (*e.g.,* CNSSI 1253).

Furthermore, the AFG content presents pointers to Defense Knowledge Online (DKO) Knowledge Centers that contain systems engineering guidance, standards, lessons learned, and examples. The DKO Knowledge Centers are organized under the six OCAs (see Figure 1), plus a Foundational (FND) IA category to capture fundamental IA constructs. Systems engineering details will evolve as guidance and standards emerge (many are still under development), and as the community posts lessons learned and examples for the benefit of others.

IA Guidance Scope and Precedent

DoD acquisition programs may use DoDI 8500.2 to determine the mission assurance category (MAC) and Confidentiality Level (CL) of the deliverable system. The MAC and CL together provide a scope of relevant security controls with respect to the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP). The AFG presents GIG IA Architecture guidance associated with DoDI 8500.2 security controls to promote taking the first steps toward achieving an assured GIG. Those controls stated within GIG IA Architecture not appearing in DoDI 8500.2 become points of discussion within the acquisition program. Acquisition programs should address all GIG IA Architecture guidance, even if they choose not to implement all guidance.

Addressing all guidance ensures conscious omission with rational justification; this is preferable to omission by oversight. There are four options to *address* AFG guidance. Ascertain which guidance is applicable to your situation and—

- Describe what you will do or acquire to satisfy the guidance,
- Describe an external dependency on a solution that will satisfy that guidance (*e.g.* leverage an enterprise service) and the means by which this dependency is agreed upon, *e.g.* service level agreement (SLA), memorandum of understanding (MOU), *etc.*
- Describe which guidance will not be met (no action taken) and provide a rationale regarding how the resulting risk will be managed.
- Address the guidance by stating it is not applicable (NA) to your situation and provide a rationale regarding how the resulting risk will be managed; and, verify the NA decision with the Designated Approving Authority (DAA).

AFG as a Methodology

AFG is a methodology for use by acquisition programs and operations to objectively plan and assess their alignment with GIG IA Architecture.

AFG Guides and Templates

The AFG provides a framework that serves as a foundation to define tools and templates for GIG IA Architecture (or assured NC) planning, assessing, tracking, and reporting.

Overview Documents

The Overview documents provide details about AFG from various perspectives—

- AFG User Guide—provides direction on how to use AFG
- AFG Business Overview—provides a business overview for managers and executives
- AFG In Depth View—contains many details on the background and motivation for AFG.

Planning Documents

The Planning documents instruct users on how to perform planning for GIG IA Architecture alignment—

- AFG Planning Guide
- AFG Planning Template
- AFG Content
- AFG Traceability.

Users can read the AFG Planning Guide for direction on how to use the AFG Content to populate the AFG Planning Template; and the AFG Traceability document to find associated DoDI 8500.2 and DCID 6/3 controls.

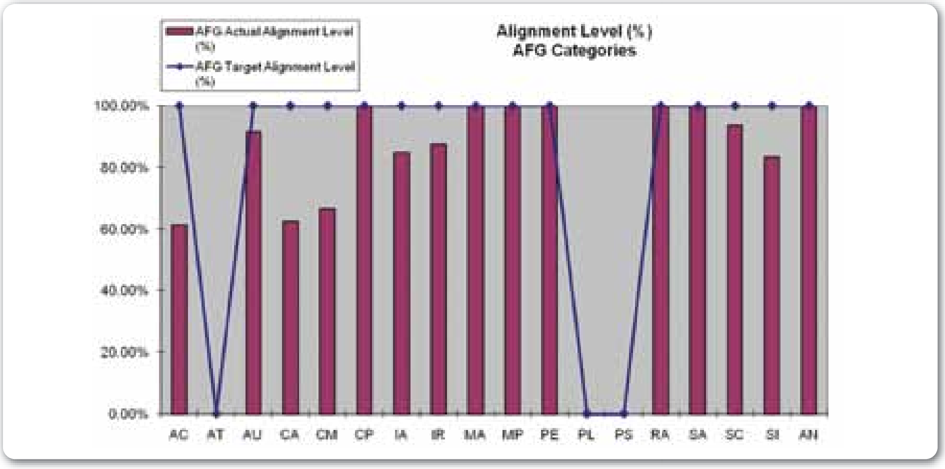


Figure 3 Sample AFG Assessment Graph

Assessment Documents

The Assessment Documents instruct users on how to perform assessments of GIG IA Architecture alignment—

- AFG Assessment Guide
- AFG Assessment Report Template
- AFG Assessment Tool.

Users can read the AFG Assessment Guide to obtain direction on how to use the AFG Assessment Tool to populate the AFG Assessment Report Template. Figure 3 shows a sample output from the AFG Assessment Tool, with the blue line representing a target alignment level and the bars representing the actual alignment level against the target.

AFG Users

Primary users of AFG are systems security engineers who plan and assess the IA posture of an operation or an acquisition program. AFG provides a method to streamline the association of assured NC guidance (enterprise focus) with security controls (system or program focus).

AFG Consumers

The primary consumers of AFG output are the Program Managers, Portfolio Capability Managers, executives, and ultimately the Component CIO organizations for DoD, and the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/DoD CIO, which includes the DIAP.

Conclusion

NSA IAD's Enterprise IA Systems Engineering Services Office published AFG v1.0 30 September 2008. This first version is the result of a year of discussion among NSA, DIAP, and DISA staff, and volunteers from the Military Services, whom the authors would like to thank for their time and dedication. We welcome and count on input from the DoD, Intelligence, and National Security Systems Communities to evolve and improve the AFG. ■

References

1. DCID 6/3 was superseded by *Intelligence Community Director (ICD) 503 Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation* on 15-Sep-2008. Reference to DCID 6/3 herein is due to its familiarity to the community.
2. As of this writing, the release of CNSSI 1253 v1.0 pending review of the latest draft v5.0.
3. Web: *http://www.defenselink.mil/cio-nii/infoassurance/diap.*
4. Defense-Wide Information Assurance Program. *http://www.defenselink.mil/cio-nii/infoassurance/diap*
5. Alignment Framework for GIG IA Architecture v1.0. *https://www.us.army.mil/suite/folder/9214521*
6. GIG IA Architecture v1.1 16 November 2006. *https://www.us.army.mil/suite/kc/13000401.*
7. Net Centric Operations Conceptual Framework. *http://www.oft.osd.mil/initiatives/ncw/ncw.cfm.*
8. Joint Capability Areas. *http://www.dtic.mil/futurejointwarfare/index.html.*
9. CJCSI 6212.01 Interoperability and Supportability of Information Technology and National Security Systems. *http://www.dtic.mil/cjcs_directives/cjcs/instructions.htm.*
10. CNSSI 1253 Security Controls Catalog. *http://www.cnss.gov.*

About the Authors

Keith D. Willett | with 25 years of experience in information technology and information assurance, Mr. Willett currently supports the NSA Enterprise IA Systems Engineering Services Office. Mr. Willett is an author and teacher of Information Assurance and recently published *Information Assurance Architecture via* Auerbach Publishing in June 2008. He may be reached at *kwillett@mitre.org.*

Stephen G. York, MBA, PMP | In his role as Integration Lead for the Enterprise IA Systems Engineering Services Office of the National Security Agency, Mr. York's primary focus is the adoption of GIG IA Architecture and assured net-centricity into the Defense Acquisition process. Drawing upon a 20+ year background in Defense Acquisition, Program Management, and Knowledge Management, Mr. York also leads the integration efforts required for the incorporation of GIG IA principles into emerging enterprise architectures. He may be reached at *sgyork@missi.ncsc.mil.*

Carnegie Mellon University CyLab

by Angela Orebaugh

CyLab is a university-wide, multidisciplinary initiative involving more than 200 faculty, students, and staff at Carnegie Mellon that builds on more than two decades of Carnegie Mellon's leadership in information technology. [1] CyLab works closely with the CERT Coordination Center (CERT/CC), a leading, internationally recognized center of Internet security expertise.

Carnegie Mellon, established in 1900, is a global research university located in Pittsburgh, PA. It is currently home to more than 10,000 students, 70,000 alumni, and 4,000 faculty and staff. CyLab is a university-wide, multidisciplinary initiative involving more than 200 faculty, students, and staff at Carnegie Mellon that builds on more than two decades of Carnegie Mellon's leadership in information technology. [1] CyLab works closely with the CERT Coordination Center (CERT/CC), a leading, internationally recognized center of Internet security expertise. Through its connection to the CERT/CC, CyLab also works closely with US-CERT—a partnership between the Department of Homeland Security's National Cyber Security Division (NCSD) and the private sector to protect our nation's Internet Infrastructure.

CyLab's goal is to build mutually beneficial public-private partnerships to develop new technologies for measurable, available, secure, trustworthy, and sustainable computing and communication systems and to educate individuals at all levels. CyLab provides technology resources and expertise in four areas—

- Technology transfer to and from the public sector
- Technology transfer to and from the private sector
- Development of Information Assurance professionals
- National awareness programs and tools.

Cylab has designated the following key areas of research and development, spanning a wide range of technologies, systems, and users—

- **Mobility**—Conduct research and development to create a more secure mobile environment in its current state and design and implement new, innovative technologies, networks, and systems that will securely empower future users.
- **Next-Generation Secure Internet**—Conduct R&D to build the next generation Internet, a global, ubiquitous communication network in which users, human or otherwise, can access the services they want, when they want, with confidence that those services are functioning properly, and without fear of interference.
- **Available and Secure Networks and Communications**—Conduct R&D of new applications and methods to support and secure network communications, including encryption, sensor development and deployment, modeling and response technologies, and threat analysis.
- **Secure Home Computing**—Conduct R&D that contributes to the growth and security of the digital home, including networked devices, home computers, and storage for personal devices (*e.g.*, Apple's Internet Pod [iPod] or the digital video recorder [DVR]).

- **Access to Devices and Spaces**—Conduct R&D in innovative technologies and methods that empower user-controlled access, and identify and quantify the desirability of individuals seeking access. CyLab access research, including smart phones that control door locks, iris detection, and face recognition, is currently applied in numerous military and law enforcement environments.
- **Available and Secure Computing Systems**—Conduct R&D of computing systems for critical applications that are resilient to accidental faults and intentional attacks, and develop new technologies, models, methods, or policies that support secure and accessible systems.
- **Trusted Computing**—Conduct research in secure application design on trusted hardware, software-based attestation, and policies and methods for trusted computing environments.
- **Protecting Privacy and Confidentiality of Personal Information**—Conduct R&D of tools and methods that support privacy protection at the organizational and individual levels.

The National Security Agency (NSA) designated Carnegie Mellon as a Center of Academic Excellence in Information Assurance Education (CAE/IE). The Information Networking Institute (INI) at Carnegie Mellon is the education partner of CyLab. [2] The following are some of Carnegie Mellon CyLab's education initiatives—

- **Professional Graduate Degree Programs**—include programs addressing networking and security, offered through the INI—
  - MS in Information Security Technology and Management (MSISTM)
  - MS in Information Networking (MSIN)
  - MS in Information Technology-Information Security (MSIT-IS).
- **Executive Education Programs—** provide executives and senior managers with professional services and skills to enhance their effectiveness and career progression.
- **Capacity Building Programs**—include the Federal Cyber Corps Scholarship for Service (SFS) program and an Information Assurance Capacity Building Program for Minority Serving Institutions.
- **Awareness and Outreach Programs** —educate and inform the general populace and professionals about cyber security and promote safe and responsible online behavior. Examples include the MySecureCyberspace Portal and Game at *www.mysecurecyberspace.com*.

CyLab maintains a number of global initiatives for research and education including the following—

- **Carnegie Mellon CyLab Athens**—a partnership with Athens Information Technology (AIT) in Athens, Greece.
- **International Collaboration for Advancing Security Technology (iCast) Taiwan**—a program that the Taiwan government sponsored to develop advanced technologies for Security Operation Centers (SOC), remote authentication, and software security and to enhance the research and education capabilities in Taiwan.
- **Carnegie Mellon CyLab Japan**—a partnership with Hyogo Institute of Information Education Foundation, offering the MS in Information Technology-Information Security (MSIT-IS) degree in Kobe, Japan.
- **Athens MSIN**—a partnership with Athens Information Technology (AIT) offering the MSIN degree in Athens, Greece. ■

References

1. For more information on CyLab, please refer to *http://www.cylab.cmu.edu.*
2. For more information on the Information Networking Institute, please refer to *http://www.ini.cmu.edu.*

About the Author

Angela Orebaugh | supports a variety of security engagements with the National Institute of Standards and Technology (NIST). She has 15 years of experience in information technology and security and is the author of several technical security books including Nmap in the Enterprise and Wireshark & Ethereal Network Protocol Analyzer Toolkit. Ms. Orebaugh is also an adjunct professor at George Mason University. She may be reached at *iatac@dtic.mil.*

Carnegie Mellon University CyLab SME

by Angela Orebaugh

This article continues our profile series of members of the Information Assurance Technology Analysis Center (IATAC) Subject Matter Expert (SME) program. Carnegie Mellon's Cylab—a center for cyber security research and education—provides vital research in new technologies and emerging issues and trends. The 2008 CyLab Annual Partner's Meeting provided faculty updates on cutting edge research in the following critical areas—

- Mobility
- Access to Devices and Spaces
- Business Risks
- Secure Software Engineering
- Security Economics
- Trustworthy Computing
- Protecting Privacy and Confidentiality of Information.

This article highlights some of the research and subject matter experts for each of the critical areas.

Dr. Adrian Perrig is an Assistant Professor in Electrical and Computer Engineering, Engineering and Public Policy, and Computer Science. Dr. Perrig's research interests revolve around building secure systems and include Internet security, security for sensor networks and mobile applications. In the Mobility session, Dr. Perrig presented a new protocol, Gather, Authenticate 'n Group Securely (GAnGS) for the secure exchange of authentication information among a group of people. GAnGS resists group-in-the-middle and Sybil attacks by malicious insiders, as well as infiltration attacks by malicious bystanders. GAnGS has been implemented and evaluated on Nokia N70 phones.

Dr. Raj Rajkumar is a Professor in Electrical and Computer Engineering. His current research projects include the FireFly wireless sensor networks effort, resource kernels for guaranteed enforcement of throughput and timeliness in distributed real-time operating systems, vehicular networks, methodologies for model-based design and development, and autonomous vehicles. In the Access to Devices and Spaces session, Dr. Rajkumar presented complementary efforts designed to provide and enhance physical security and surveillance, including FireFly and Sensor Andrew. The Firefly family of sensor networks is used to sense, monitor, and control aspects of the physical environment including real-time tracking of personnel in safety-critical areas and valuable assets. The Sensor Andrew is a large-scale deployment of sensor networks, deployed across four campus buildings that integrates different sensors, actuators, and applications.

Ms. Dawn Cappelli is an adjunct professor and the technical lead for the CERT insider threat research, including the Insider Threat Study being conducted with the US Secret Service National Threat Assessment Center. In the Business Risks session, Ms. Cappelli presented on the Common Sense Guidelines to Prevention and Detection of Insider Threat. The findings are based on the analysis of over 350 prosecuted cases of insider crimes that have taken place from 1996 to 2007. The presentation provided detailed, actionable steps to better manage the risk of insider threat.

Dr. Anupam Datta is a Research Scientist focused on high assurance for secure systems. His current research includes a framework for modeling and analysis at two levels of abstraction: system architecture and system implementation. The target application domain includes deployed and industrial standard contemporary systems such as virtual machine monitors (VMMs), and co-processor-based systems such as those utilizing the Trusted Computing Group's Trusted Platform Module (TPM). In the Secure Software Engineering session, Dr. Datta presented on two ongoing efforts—the Logic of Secure Systems (LS^2) and its application to trusted computing, and model-checking methods for secure systems with application to a security hypervisor.

Dr. Alessandro Acquisti is an Assistant Professor in Information Technology and Public Policy. His research investigates the economic and social impact of IT, and in particular the interaction and interconnection of human and artificial agents in highly networked information

▷▷ continued on page 24

The Insider Threat to Information Systems—An IATAC State-of-the-Art Report

by Karen Goertzl

"We forget cruelty and past betrayal, Heedless of where the next bright bolt may fall" [1]

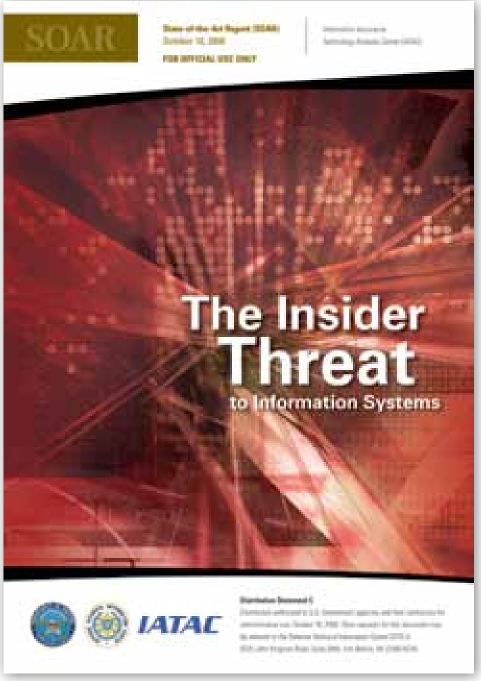
The Information Assurance Technology Analysis Center (IATAC) has just published *The Insider Threat to Information Systems—A State-of-the-Art Report*, which provides a comprehensive look at the most significant of today's efforts in government, industry, and academia to detect and combat the wide variety of insider threats to operational information systems and to the information technology supply chain.

It appears to be in our nature to place more trust in those people that we know. For this reason, most information security programs focus on keeping unauthorized outsiders from accessing our information systems. Although a real threat is posed by outside attack, insiders, because of their positions of trust, are often in a better position to cause us harm. This trust of insiders, at least some individuals, is not always warranted, and their insider access combined with malicious (or accidental) actions can cause damage to our organizations that often dwarfs the damage potential of outsiders. Insider incidents can prove extremely costly financially, in terms of reputation, or worse, in terms of loss of life.

Generally speaking, an insider is a person within an organization who is entrusted with privileges to access the organization's information, information systems, and/or facilities. In some cases, an individual who previously held such privileges but no longer does so may also be considered an insider. When an insider abuses these privileges to hinder resources or impede the mission of an organization, it is referred to as an insider attack. The insider's actions are governed by a wide range of motivations that vary by sector and institution. Within financial services organizations, the most common motivations are greed, revenge, disgruntlement, and ego. Within other organizations, especially government, ideology can be a major factor.

Determining the level of the insider threat has been difficult because of a widespread reluctance of organizations to report insider incidents. Although a lot of research has been done to categorize and model the insider threat, much of this research has been derived from what is suspected concerning the threat. Still, a growing body of knowledge has been derived from the collection of incidents that have been publicly acknowledged, which has driven managers across public and private sectors to work to develop both knowledge of insider threats within their organizations and training and technical countermeasures.

The insider threat has affected all parts of the community, including public and private sectors in a variety of industry segments and communities of interest. However, approaches to addressing the problem vary depending on the perspectives of the various stakeholders. This variance has influenced the development of anti-insider threat solutions specific to each industry's individual requirements. The national security sector has primarily focused on the threat induced by the introduction of malicious code, unauthorized access to data, exfiltration of sensitive data, alterations in system activity, and



alterations to system topology. This sector relies heavily on traditional counterintelligence and information assurance programs to protect against these threats but has also been working to adopt new technologies and strategies to monitor, detect, prevent, and recover from insider threats. Efforts have included recent acquisition of a multipart technical solution that includes host and network anomaly detection capabilities, a correlation engine to analyze the anomaly data, and a tool to allow detailed monitoring of hosts that have previously been flagged for unusual or suspicious behaviors. Within the public sector, insider threat mitigation often conflicts with public pressure to increase efficiencies and decrease operating costs. In addition, privacy concerns are more prevalent, complicating the implementation of technical monitoring controls. Actual approaches vary dramatically by industry and organization but in general are weighted heavily toward policy-driven approaches.

Insider threat solutions from the vendor community and academia are evolving. Several categories of dedicated insider threat, insider computer fraud, and data exfiltration mitigation products have begun to emerge in the commercial marketplace and are characterized as advancing the state of the art in insider threat mitigation. While many of these products are intrusion detection system (IDS) like technologies focused inward, the trend is now toward use of products that focus on host-level activities, including behavior profiling to help differentiate between accidental misuse and true malicious insider activities. Some products also look at behavior profiles that help identify the passive insider. Academics are also engaged in a wide range of insider threat mitigation research projects, with some institutions devoting full-time research staff to the problem. Their activities range from gaining a better understanding of the motivations of insiders to identification of precursors to attacks by insiders.

To address the proliferating (and justified) concern regarding the insider threat to information systems, the IATAC has just published *The Insider Threat to Information Systems—A State-of-the-Art Report (SOAR)*, which provides a comprehensive examination of the current state of the art in addressing the insider threat as it pertains to information technology systems. This SOAR provides an overview of how the insider threat is defined and viewed across government, industry, and academia, and discusses the different policy, technical, and procedural approaches being applied by each of these communities to address the threat. The SOAR also describes ongoing research meant to further our ability to limit or prevent insider attacks. Finally, the report presents a compendium of current state-of-the-art best practices being used in government and industry to mitigate insider threats.

The Insider Threat to information Systems, which is Unclassified/For Official Use Only, is releasable to government organizations and authorized contractors, and to others upon application to the Defense Technical Information Center. This SOAR can be obtained through the IATAC website *http://iac.dtic.mil/iatac/form.html* or it can be downloaded from TEMS (Total Electronic Migration System) at *http://iac.dtic.mil/iatac/TEMS.html.* ■

References

1. Robert Graves. *The White Goddess: A Historical Grammar of Poetic Myth.* (London, UK: Faber & Faber, 1948).

About the Author

Karen Goertzl | has 24 years in IA, software assurance, and net-centric architectures and applications. She supports the Department of Homeland Security and ASD(NII) as a software assurance subject-mater expert, and was lead technologist for 3 years on DISA's Application Security Program. She also leads ASD(NII)'s effort to define an approach for two-level GIG network management. In 2004, she authored *IAnewsletter* articles on Autonomic Computing and Computer Immunology. Previously, she was a CDS engineer for Getronics (now BAE/DigitalNet). For Wang and Honeywell she consulted to DoD, Civil agencies, and NATO on security architecture and policy, risk management, COOP, and software development.

Army, Navy, Air Force, and Cyber—Is it Time for a Cyberwarfare Branch of Military?

by LTC Gregory Conti and COL John "Buck" Surdu

The Army, Navy, and Air Force all maintain cyberwarfare components, but these organizations exist as ill-fitting appendages that attempt to operate in inhospitable cultures where technical expertise is not recognized, cultivated, or completely understood. The services have developed effective systems to build traditional leadership and management skills.

Disclaimer

The views expressed in this article are those of the authors and do not reflect the official policy or position of the US Military Academy, the Department of the Army, or the US Government.

At critical points in history, technological advances have driven fundamental changes in the conduct of warfare. The tank, radio, long bow, helicopter, machine gun, military robot, and unmanned aerial vehicle, among many other technologies, changed the face of warfare. Agile military organizations exploited these new technologies—by adopting innovative tactics, doctrine, cultures, and organizations—or faced irrelevance and probable defeat on the battlefield. However, occasionally, a new technology is so significant that it creates a discontinuity in the conduct of war that necessitates creation of an entirely new military service. This situation occurred in the United States, resulting in the formation of the Air Force in 1947. The advent of air power fundamentally altered the conduct of warfighting and drove the transformation of the Army Air Corps into the United States Air Force.

The revolution in cyberwarfare places today's militaries at a similar cusp in history and necessitates the formation of a cyberwarfare branch of the military, on equal footing with the Army, Navy, and Air Force. We do not make this recommendation lightly—the time is now to reevaluate the structure, organization, and missions of today's armed forces in order to succeed in the Global War on Terrorism, ensure victory in future conflicts, and avoid technological surprise. This article asks and seeks answers to hard, but necessary questions regarding cyberwarfare and the future of our armed forces.

To understand the compelling need to create a cyberwarfare service, it is useful to examine the missions of the existing United States Armed Forces—

- The Army's mission is to fight and win our Nation's wars by providing prompt, sustained land dominance across the full range of military operations and spectrum of conflict in support of combatant commanders. [1]
- The mission of the Navy is to maintain, train, and equip combat-ready Naval forces capable of winning wars, deterring aggression and maintaining freedom of the seas. [2]
- The mission of the United States Air Force is to fly, fight and win…in air, space, and cyberspace. [3]

Of these three, only the Air Force mission mentions cyberspace. This reference was added to the Air Force mission statement in 2006, with the creation of the two-star Air Force Cyber Command provisional [AFCYBER (P)], [4] [10] and while acknowledgement of cyberspace as a core military mission by the Air Force is an admirable step

forward, it is not the solution. The importance and mission requirements of cyberwarfare are larger than any existing service organization. More importantly, the cultures of the Army, Navy, and Air Force are fundamentally incompatible with that of cyberwarfare. These existing services operate in the kinetic arena, the directed application of physical force, whereas cyberwarfare exists in the non-kinetic world of information flows, network protocols, and hardware and software vulnerabilities. [5] Both kinetic and non-kinetic operations are critical components of warfighting, and the current ad hoc solution of small pockets of cyberwarfare capability within the existing services is not as effective as it could be.

The Army, Navy, and Air Force all maintain cyberwarfare components, but these organizations exist as ill-fitting appendages that attempt to operate in inhospitable cultures where technical expertise is not recognized, cultivated, or completely understood. The services have developed effective systems to build traditional leadership and management skills. They are quite good at creating the best infantrymen, pilots, ship captains, tank commanders, and artillerymen, but they do little to recognize and develop technical expertise. As a result, the Army, Navy, and Air Force hemorrhage technical talent, leaving the Nation's military forces and our country under-prepared for both the ongoing cyber cold war and the likelihood of major cyberwarfare in the future. One need only review the latest computer security report card, which gave the Federal Government an overall grade of C, and the Departments of Agriculture, Commerce, Defense, Interior, Treasury, Transportation, and Veterans Affairs a grade of D or lower, to understand our nation's vulnerability. [6]

The Ongoing Cyber Cold War

Make no mistake—the cyber cold war is being waged now. The networks and information processing assets of all branches of the United States Government are under continual attack. In 2007, 1,500 computers in the Department of Defense were taken offline because of a cyber attack. According to Defense Secretary Robert Gates, the Pentagon alone receives hundreds of attacks per day, many from nations that are supposed to be our "friends." Similarly, the Department of Homeland security acknowledged more than 800 attacks in the past two years. Every component of our country, including government, industry, defense, and individual citizens, is becoming increasingly dependent on technology. A successful, major cyber attack could paralyze our country and its armed forces. Such an attack is not idle speculation. The first cyberwar has already occurred. In 2007, the technologically advanced country of Estonia was paralyzed by waves of attacks, suspected to be of Russian origin, that targeted key information assets, including those of Estonia's banks, major media outlets, and government agencies. Both the United Kingdom and United States are facing repeated attacks that some experts attribute to the Chinese Liberation Army. [7] Attacks, such as those faced by Estonia, the United Kingdom, and the United States are harbingers of other more devastating attacks sure to come.

Cyberwarfare is fundamentally different from traditional kinetic warfare. National boundaries in cyberspace are difficult, if not impossible, to define. Lawyers and pundits are still debating the formal definition of an "act of war." Asymmetries abound and defenders must block all possible avenues of cyber attack. An attacker need only exploit a single vulnerability to be successful. A lone, but specially crafted, phishing e-mail sent to a senior official could compromise an entire network. Attackers can assault objectives from virtually any point on the planet, hopping through a number of intermediate points to mask their trail. Verifying the source of network attacks is a difficult and sometimes impossible task.

The skill sets required to wage cyberwar in this complex and ill-defined environment are distinct from waging kinetic war. Both the kinetic and non-kinetic are essential components of modern warfare, but the status quo of integrating small cyberwarfare units directly into the existing components of the armed forces is insufficient. A separate military service to conduct cyberwarfare must be created. Adding an efficient and effective cyber branch alongside the Army, Navy, and Air Force would provide our nation with the capability to defend our technological infrastructure and conduct offensive operations. Perhaps more important, the existence of this capability would serve as a strong deterrent for our Nation's enemies.

A Clash of Cultures

The cultures of today's military services are fundamentally incompatible with the culture required to conduct cyberwarfare. This assertion in no way denigrates either culture. Today's militaries excel at their respective missions of fighting and winning in ground, sea, and air conflict; however, the core skills each institution values are intrinsically different from those skills required to engage in cyberwarfare. Cyber requires a deep understanding of software, hardware, operating systems, and networks at both the technical and policy levels. The Army, Navy, and Air Force are run by their combat arms officers, ship captains, and pilots, respectively. Understandably, each service selects leaders who excel at conducting land, sea, and air battles and campaigns. A deep understanding and respect for cyberwarfare by these leaders is uncommon.

To understand the culture clash evident in today's existing militaries, it is useful to examine what these services hold dear—skills such as marksmanship, physical strength, and the ability to jump out of airplanes and lead combat units under enemy fire. Accolades are heaped upon those who excel in these areas. Unfortunately, these skills are irrelevant in cyberwarfare. Consider two events, the Best Ranger competition conducted by the Army at Fort Benning, Georgia, and the Capture the Flag contest that occurs each year at the DEFCON hacker conference. Akin to an Iron Man competition, the Best Ranger competition is a career-long achievement recognized across the Army. The winning team proves it has the fortitude to meet intense physical demands. Capture the Flag, on the other hand, brings together some of the world's best hackers in similarly intense competition. Earning a "black badge" as the winning team at DEFCON represents a similar accomplishment, but would pass unrecognized by today's military services. Both require years of preparation—one accomplishment is intensely valued, but the other is not. We are not arguing that there is anything wrong with the Best Ranger competition or similar events. They have proven effective in creating the combat forces necessary to conduct a broad spectrum of operations. We are, however, arguing that similar competitions and accolades are needed to reward those who will be the heroes in a future cyber battle or campaign.

The culture of each service is evident in its uniforms. Consider the awards, decorations, badges, patches, tabs, and other accoutrements authorized for wear by each service. Absent is recognition for technical expertise. Echoes of this ethos are also found in disadvantaged assignments, promotions, school selection, and career progression for those who pursue cyberwarfare expertise, positions, and accomplishments. Some cyberwarfare soldiers, sailors, and airmen who seek to make a career of the military go to great lengths to mask their technical expertise and assignments from promotion boards by making their personnel evaluations appear as mainstream as possible. It is also common for technically oriented career fields to create entire artificial unit hierarchies that mirror combat arms units to help prevent prejudice and retribution. Evidence to back these assertions is easy to find. From a recent service academy graduate who desired more than anything to become part of a cyberwarfare unit but was given no other option than to leave the service after his initial commitment, to the placement of a service's top wireless security expert in an unrelated assignment in the middle of nowhere, to the PhD whose mission was to prepare PowerPoint slides for a flag officer—tales of skill mismanagement abound.

The realities of the existing services' career environment and culture is not lost on their technical experts, many of whom choose to leave military service to pursue their passion. Do technologists believe in serving their country and serving in the military? Many do, but we must create an environment where their expertise is valued, cultivated, and rewarded, else they will take their skills elsewhere. We are not arguing that the cultures extant in the services are not effective in creating the skills needed for a broad spectrum of operations, both conventional and unconventional. Instead, we are arguing that these cultures inhibit (and in some cases punish) the development of the technical expertise needed for this new warfare domain. Given the entrenched values, personnel systems, leadership, and culture, only creation of a new military service from the ground up would allow an environment capable of recruiting, retaining, training, and grooming the cyberwarfare capabilities and personnel our nation desperately needs. For these reasons, we are arguing that the time is right to create a new service focused on cyberwarfare and its interactions with, and support of, the other services in the conduct of more traditional operations.

A key question when forming a cyber branch of military service is whether the National Security Agency (NSA) is already such a force today. NSA seeks to recruit top-tier talent in a wide range of technical disciplines, including computer science, electrical engineering, mathematics, cryptanalysis, and signals analysis. [8] Much of NSA's work is classified, but it falls into two broad missions—information assurance and signals intelligence. [9] However, NSA suffers as a result of the cultures of the Army, Navy, and Air Force. NSA's long-term civilian workforce trains the soldiers, sailors, and airmen, particularly those of mid-career ranks, who rotate into an NSA assignment, only to lose them after a few short years. Technical skill sets atrophy quickly, and many service members rotate to unrelated fields where they lose their expertise. As a result, NSA is constantly training and then losing military personnel, placing a significant burden on its civilian workforce. The problem is compounded because repeated assignments to NSA and similar organizations are not valued by the services, and those service members who excel at cyberwarfare activities face significant risks to their careers.

Fundamentally, we believe that while today's mission and capabilities of NSA overlap to some degree with those of a military cyberwarfare branch, NSA is not the right type of organization. Led by a three-star flag officer, NSA is relegated to a subordinate role when the mission of cyberwarfare should be on par with the other military services. Ultimately, the role of fighting and winning in cyberspace is a military mission, which demands a military organization—one that can recruit, train, and retain highly qualified cyberwarfare combatants.

A Path Forward

The Air Force is heading in the right direction. Its drive toward a cyberwarfare capability is admirable. However, its initiative needs to extend beyond the Air Force to encompass the entire military. The Air Force's engagement of Slashdot.org, probably the most popular technical news source and discussion forum for the technical community, was the right move. Only by understanding the culture of the technical workforce can a cyberwarfare organization hope to succeed—cultural change must occur in order to maximize our cyberwarfare capabilities. High-and-tight haircuts, morning physical training runs, rigorously enforced recycling programs, unit bake sales, and second-class citizen status are unlikely to attract and retain the best and brightest people.

Cyberwarfare requires unique technical skills as well as skills in creative problem solving, poise under pressure, and critical thinking. Attributes that are desirable in soldiers, such as physical endurance, marksmanship, and technical skills associated with the employment of traditional forces and weapons systems, do not translate well to cyberwarfare. Instead, skills such as the ability to scan through logs and reports to quickly ascertain the nature and threat of a cyber battle, knowledge of the latest network exploitation techniques and attack tools, and a deep understanding of information flows are the skills needed in a cyber corps operator. While some required traits are similar to today's military forces, such as integrity, teamwork, dedication to mission, the ability to keep secrets, and creative problem solving under pressure, many are fundamentally different. Because the skill sets and mission areas are different, the cyber corps needs to recruit, train, and retain a different breed of warrior. Institutions such as ROTC should be reevaluated to determine their usefulness as a mechanism for staffing our proposed cyberwarfare service. Appropriate training exercises, such as network attack-and-defend exercises, will also need to be created that fit cyberwarfare mission requirements. In short, creating a new cyber service provides the opportunity to rethink kinetic warfare paradigms, adapting some, discarding others, and creating new non-kinetic warfare tactics and strategies.

Personnel with the technical expertise required for cyberwarfare are in high demand. Competitive salaries are always beneficial but not necessarily a requirement. Consider Google. Google has recruited some of the world's best talent in a variety of technical disciplines, not through excessive salaries, but by creating a culture where people want to work. The idea of working on interesting problems, experimenting with cutting-edge technical gear, spending 20 percent of one's time working on a project of one's own choosing, and interacting with similarly talented people has made Google an A-list employer that must turn away qualified applicants. While a cyberwarfare branch's model would likely be different, the key idea is the same—make it the most desired place to work in the computer security community.

Recruiting ethical, trustworthy people is, of course, of paramount importance. In their formative years, many technically talented individuals make critical decisions that influence the direction of their life. In the hacking community, perhaps the most important decision is whether or not to engage in illegal activity. By creating a cyber organization that is elite, complete with role models that junior members would want to emulate, we can recruit individuals before they make irreversible decisions that would eliminate their ability to serve their country.

One key advantage is that the current services would not need to change significantly. They would only need to interface correctly. Services must be able to communicate and coordinate to conduct joint and combined operations. Correctly constructing the interfaces between each service is a key to success. The Army, Navy, Air Force, Marines, Coast Guard, and myriad federal agencies, as well as their international counterparts, successfully coordinate operations today, and cyber will be no exception.

Conclusions

The overwhelming dependence of individuals, militaries, businesses, and governments worldwide on information technologies and the catastrophic consequences of the disruption or destruction of those technologies present a clear and present danger to the United States. We are facing a severe cyberwarfare threat now—but a major cyberwar involving the United States is inevitable. Our existing military organizations' cyberwar capability is inadequate, and this situation is unlikely to change without radical transformation. The best solution is to create a new cyber service and carefully craft its organization and culture to meet current and future needs. A properly designed organization will promote intellectual agility and retain the top-tier talent required to conduct successful offensive and defensive operations in cyberspace. The change will not be easy, but the risks inherent in maintaining the status quo are significantly worse. ■

References

1. "The United States Army: Organization." *http://www.army.mil/institution/organization.*
2. Navy Organization: *http://navy.mil/navydata/organization/org-top.asp*
3. Air Force Link: *http://www.af.mil/main/welcome.asp*
4. Anne Proctor. "AF launches cyberspace task force." Air Force Print News, 6 April 2006. *http://www.af.mil/news/story.asp?id=123018708.*
5. Richard Bejtlich. "Air Force Cyberspace Report." TaoSecurity, 12 October 2007. *http://taosecurity.blogspot.com/2007/10/air-force-cyberspace-report.html.*
6. Eight Report Card on Computer Security at Federal Department and Agencies. House Committee on Oversight and Government Reform, 20 May 2008. *http://republicans.oversight.house.gov/media/PDFs/Reports/FY2007FISMAReportCard.pdf.*
7. Richard Nortonton-Taylor. "Titan Rain—how Chinese hackers targeted Whitewall." The Guardian, 5 September 2007. *http://www.guardian.co.uk/technology/2007/sep04/news.internet.*
8. "Career Fields." National Security Agency. *http://www.nsa.gov/careers/careers.cfm.*
9. "Mission Statement." National Security Agency. *http://www.nsa.gov/about/about00003.cfm.*
10. *http://afcyber.af.mil.*

About the Authors

LTC Gregory Conti | is an Assistant Professor of Computer Science at the United States Military Academy, West Point, New York. He holds a PhD from the Georgia Institute of Technology, a MS from Johns Hopkins University, and a BS from the United States Military Academy, all in computer science. His research includes information warfare, security data visualization, and web-based information disclosure. He may be reached at *gregory.conti@usma.edu.*

COL John "Buck" Surdu | is currently serving as Chief of Staff of the Army's Research, Development, and Engineering Command. He has previously served in a variety of infantry assignments, as a researcher at the Army Research Laboratory, as a senior researcher in the Information Technology and Operations Center, as a product manager for the One Semi-Automated Forces (OneSAF), and as a project manager at the Defense Research Projects Agency. In addition to a BS degree in computer science from the United States Military Academy, Col Surdu earned an MBA from Columbus State University. Col Surdu later earned a MS in computer science from Florida State University, focusing on artificial intelligence. He completed his formal education with a doctoral degree in computer science from Texas A&M University focusing on simulation technology and its applications to command and control. He may be reached at *john.surdu@us.army.mil.*

Letter to the Editor

Q ***I understand there is a new way to share research & development (R&D) information across government, industry and academia. Can you provide some information on the project?***

A DoD Techipedia is a Department of Defense (DoD) sponsored wiki service on DoD scientific and technical information (S&T) available to all government and authorized commercial and academic institution personnel. DoDTechipedia was developed to provide an agile means to increase collaboration and communication among the R&D DoD, government, commercial enterprise, and academic community.

From DoDTechipedia's home page, you can navigate to areas such as acronyms, terminology, technology areas, interest areas, organizations, how to do business, and private and public blogs. Within each technology area, you will find hot topics, key documents, and other information important to that technology area. For example, the information assurance (IA) technology area has included hot topics on IPv6, Software Protection, and Service Oriented Architecture (SOA) Security.

DoDTechipedia is a valuable source of information and technology that will enable users to see and discuss the innovative technologies being developed throughout the DoD and also emerging technologies across the private sector and academic institutions.

Access to DoDTechipedia requires DTIC user registration at *http://www.dtic.mil/dtic/registration* and is located at *https://www.dodtechpedia.mil/dodwiki.* ■

SCAP for the Enterprise?

by Allan Carey

Over the past couple of months, the term "SCAP" has come up in conversations with industry organizations. By now almost all government employees have heard of SCAP and, more so, FDCC (Federal Desktop Core Configuration) which has been a significant driver to SCAP awareness. I think if you asked most information security practitioners in private sector organizations about their recognition of the Security Content Automation Protocol (SCAP), they would have little to no knowledge of the standard. The following description is from NIST [1] —

The Information Security Automation Program (ISAP) is a US government multi-agency initiative to enable automation and standardization of technical security operations. The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance). NVD is the US government content repository for ISAP and SCAP.

Some large enterprises are starting to investigate SCAP to determine if it is a good fit to standardize their vulnerability management program. Industry and government alike have a similar challenge where vulnerability data come in from various sources and various formats. Some times it arrives in CVE format, others with CVE and CVSS weighting, and many vendors have their own proprietary format. Complexity around the different formats makes it nearly impossible to rationalize the data to gain a common view of an organization's vulnerability exposure.

Mentioned earlier, FDCC and OSD Computer Network Defense Pilot initiative are helping to drive awareness and adoption of SCAP. These use cases and others are accounting for rapid change in organizations. Gaps identified during the implementation of such policies are being utilized to advance current standards within SCAP and develop complimentary standards for SCAP.

Two common misperceptions in industry are that SCAP is not flexible enough to handle the exceptions experienced by industry and is not suitable to handle international scale. First, SCAP is policy agnostic and more of a reference framework/standard than edict. eXtensible Configuration Checklist Description Format (XCCDF) allows for exceptions, multiple profiles, and overrides within one common document. In addition, CVSS is meant to be flexible so organizations may leverage their own policies or standards. NIST National Checklist Program contains currently available checklist content which is contributed by both government and industry participants. Second, SCAP is designed and built to be agnostic on many fronts. The use of standard XML enables SCAP to handle international languages and, therefore, support global operations.

Another challenge is getting vendors to submit their results and information in a common format such as CVE and CVSS. A list of vendors exists at National Vulnerability Database [2] (NVD) who currently work with CVE and CVSS at a minimum to be able to understand and share information and meet a minimum set of requirements. SCAP is not in a position, however, to fully address the problem set in today's version. Additional enumerations, such as Common Configuration Enumeration (CCE), Common Platform Enumeration (CPE), and Common Weakness Enumeration (CWE), are strongly needed to standardize across and provide better vulnerability coverage.

SCAP is proving to be a durable standard with great benefit and applicability outside the government sector which can only enhance the ability to share information in public/private partnership. In the near term, SCAP has both Government commitment and financial funding; in addition, more awareness and international exposure will ensure its longevity. ■

References

1. Web: *http://nvd.nist.gov/scap.cfm*
2. Web: *http://nvd.nist.gov/scapproducts.cfm*

About the Author

Allan Carey | is the Senior Vice President of Research and Product Development at IANS. In this position, he manages all research and intellectual property across the Institute. Prior to IANS, Mr. Carey spent seven years at IDC, a global provider of market intelligence and advisory services for the IT sector. He developed and managed the Security Services practice and provided in-depth analysis, intelligence and consulting on key aspects of the information security business continuity services markets. He may be reached at *acarey@ianetsec.com.*

IA Implications for Software Defined Radio, Cognitive Radio and Networks

by Capt Ryan Thomas and Lt Col Brett Borghetti

Cognitive communications includes software defined radios (SDRs), cognitive radios (CRs), and cognitive radio networks (CRNs). These devices and systems have been heralded as highly flexible communications platforms, providing intelligent wireless adaptations that will open new economic markets, increase communication efficiency, and reduce bandwidth bottlenecks.

Disclaimer

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

Information assurance (IA), the process of providing availability, authentication, integrity, nonrepudiation, and confidentiality to information, is often the last consideration when a new information system is developed. Cognitive communications includes software defined radios (SDRs), cognitive radios (CRs), and cognitive radio networks (CRNs). These devices and systems have been heralded as highly flexible communications platforms, providing intelligent wireless adaptations that will open new economic markets, increase communication efficiency, and reduce bandwidth bottlenecks. Most of the research and development (R&D) community has been investigating the technical requirements of creating such systems rather than determining how IA services will be provided. This article examines the capabilities and applications of cognitive communications devices and investigates the implications of providing IA services.

With the decreasing cost and increasing power of analog to digital (A/D) converters, digital to analog (D/A) converters, and computer processors, a new kind of radio that performs signal processing in the digital (rather than analog) domain has become feasible. These radios, known as SDRs, move most radio frequency (RF) and intermediate frequency (IF) functionality, including waveform synthesis, into software. This move allows for great flexibility in radio operation modes (called "personalities"). A classic SDR accomplishes receive functionality by using a general purpose processor to manipulate the waveforms sampled on an A/D converter into a data stream. Transmit functionality involves similar operations, with the digital waveforms modulated by a D/A converter before amplification and transmission. This is in contrast to traditional radios, which perform these tasks either with analog components or on dedicated digital hardware and have very little flexibility in the frequencies, waveforms, modulations, and information that they can transmit or receive.

Mitola [1] first proposed the CR to leverage the flexibility of the SDR by allowing radios to make intelligent, context aware decisions. CRs adapt their core functionality based on the information they are transmitting and the RF environment in which the information is being sent. CR technology has emerged as an exciting field in the area of wireless communications research, able to increase wireless performance by intelligently select and optimize radio parameters. This technology is different from existing wireless technologies (*e.g.*, wireless fidelity [WiFi] cards, cordless mics, or cordless phones). Whereas these technologies use fixed protocols with limited and predetermined adaptability, CRs leverage

the flexibility of their SDR underpinnings to intelligently select radio parameters from a large set of possible states.

In today's technological environment, radios are more than isolated pairs. Particularly for general-purpose data communications, individual radios are often part of a larger multi-hop network consisting of various other wired and wireless devices. Consequently, many of the philosophical underpinnings of CRs have been extended from the wireless connection to encompass network functionality. Networks of nodes that intelligently select and optimize network parameters based on the end-to-end network requirements are called cognitive networks (CNs). [2] A network of CRs performing this task is called a cognitive radio network (CRN).

Whereas CRs concern themselves with only coordinating radio parameters among those CRs receiving their transmissions, CRNs must coordinate network and radio parameters among multiple CRs at all network functionality areas. Working down from the network applications, examples of parameters that CRNs could modify are multimedia coder-decoders (codecs), buffer and window sizes for flow control and/or reliable transmission, routing metrics, network topologies, medium access timings, and RF parameters. CRNs modify these parameters based on what they sense in their environment (*e.g.,* signal to noise ratios, channel occupancy statistics, coding schemes, and congestion metrics). Because CRNs are composed of CRs, the environment in which the CRN makes its decisions goes beyond the dynamic RF environment of the CR. The CRN includes all aspects of the CR environment, as well as the "virtual" environment of the network, which consists of many nodes and users running various applications with their own traffic and connectivity requirements.

Cognitive communication devices show great promise in providing flexible, autonomous mechanisms to improve communication. Researchers for this technology are proposing many applications. One is dynamic spectrum access (DSA), which uses CRs to take advantage of underutilized spectrum. DSA attempts to rework the past paradigm of dividing and licensing frequency bands to particular licensees (*e.g.,* television, frequency modulation [FM] radio, or cellular phone). Under DSA, regulatory agencies such as the Federal Communications Commission (FCC) would allow large numbers of secondary users (SU) to broadcast in unused spectrum holes between bands allocated to primary users (PU) (official licensees or priority users of a frequency) or underneath the PU's interference floor.

Another application that has received attention is that of leveraging the CR/CRN waveform and protocol flexibility to ease radio and network interoperability issues. Because SDRs can take on various personalities, this application envisions radios that can automatically and seamlessly bridge between multiple legacy radio systems. Particularly for military, first responder, and safety systems, the ability to communicate among systems working on various legacy frequency bands and waveforms can be a matter of life and death.

The software aspect of SDRs is being eagerly examined as a mechanism for lowering the cost of product development and manufacturing for mass-markets. By maintaining most of the functionality in software, rather than hardware, engineers can design the hardware once and then create multiple devices via software, greatly decreasing the product development costs and R+D lifecycle times.

However, it is DSA that is garnering the most excitement and is generally viewed as the first "killer" application area for cognitive communications. Drawing from the assertion that most of the pre-licensed spectrum is lying fallow, DSA tries to leverage this underutilized resource by "overlaying" and "underlaying" signals. Overlaying signals means that frequency-time gaps of the PU's signals are filled with signals from the SU CR; underlay means SU wideband signals are broadcast in PU frequencies at very low power levels that do not interfere with the PU's signals. Other proposed techniques for sharing "gray" frequency bands with SUs, bands that are in use by PUs but not completely (*e.g.,* PU using Code Division Multiple

Access (CDMA) waveform in which orthogonal codes remain).

DSA has garnered interest for military and commercial applications. On the defense side, Defense Advanced Research Projects Agency (DARPA) has sponsored two important academic and industry partnership programs: Next Generation (XG) and Wireless Network after Next (WNaN). From a commercial policy perspective, the Federal Communications Commission (FCC) has made several spectrum management changes, including setting aside 20 Megahertz (MHz) of bandwidth to test DSA and making DSA a part of the digital television transition plans. Commercial users (*e.g.,* Google and Microsoft) are standardizing on their approach through working groups and coalitions, including the White Spaces Coalition and Wireless Innovation Alliance.

Most CR and CRN DSA schemes operate under the assumption that some functioning set of policies, devices, and behaviors exists. Even highly decentralized and market-based approaches to the sharing of spectrum assume an accepted set of "rules" by which all radios must abide. Although these expectations are not very different from those for current spectrum sharing agreements (in which PUs assume that rogue users will not interfere with their transmissions) enforcing the DSA environment might be more difficult. Under traditional spectrum sharing agreements, legitimate and illegitimate users are often fairly static, contained, and deterministic. Enforcement can use these properties to simplify the job of detecting and isolating violators. Under DSA, however, violators and legitimate users erratically appear and disappear from frequencies, with violations potentially occurring transiently over in small time/frequency quantums, making the enforcement problem much more difficult.

Considerable research in the CR field is devoted to creating self-enforcing, self-organizing DSA behaviors. The field of game theory, in particular, has been used to evaluate the behavior of the groups of self-interested radios. [3] Mechanism design, a technique of creating incentives to produce desired behaviors from a set of self-interested participants, has been proposed as a way of harnessing these instincts of the individual players of the network toward a successful DSA system. Although the problem of ensuring spectrum availability under the influence of self-interested CRs has not been solved, the research community is actively investigating this problem.

Despite some progress into dealing with self-interested CRs, dealing with "malicious" radios is less understood. Most analysis draws a line between self-interested radios and malicious radios. The different between the two can be illustrated by an example: a competition between two players. Self-interested players obey the rules of the game and try to make choices that will maximize their chance of winning. Malicious players may cheat to win or play in ways that hurt other players' chances at winning without concern for their own performance. Malicious radios accomplish their goal by exploiting flaws in the regulator policies or simply disregarding them.

One class of malicious CR is a cognitive jammer (CJ), a radio that intelligently attempts to disrupt communication based on observations from the RF environment and network environment. These radios limit availability by performing denial of service attacks in specific bands. [4] This can be performed to either steal resources (*e.g.,* spectrum) or simply create degraded service for the other CRs. Beyond traditional jamming techniques such as blanketing a region of spectrum with interference, CJs can use several higher level techniques to deny availability to CRs. Examples of these techniques are a CJ posing as a PU or producing signals designed to mislead a CR's sensors at many levels of the communication system.

One mechanism of limiting the effect of a malicious radio is to know in advance whether a transmission is coming from a trusted radio. This mechanism can be accomplished using authentication and nonrepudiation schemes. Authentication is traditionally performed in digital domain at the frame, packet, segment, or application via cryptographic techniques, but these techniques are difficult to replicate in the waveform. Weak authentication and nonrepudiation can be accomplished by using some of the properties of the transmitted signal and can be tied into the spectrum sensing capabilities of the CR.

Most spectrum sensing systems use a "detect and classify" architecture, in which the presence of a PU is detected in the spectrum and then the waveform is classified. Often detection is accomplished by energy sensing, in which spectrum is determined to be in use or not by a simple power spectral density measurement. It is difficult using this measurement alone to differentiate between a legitimate PU and a malicious radio. However, it may be possible to use second-order detection characteristics to provide authentication information (*e.g.,* the expected on/off behavior of the legitimate user). Classification gives more authentication possibilities because it can use the expected waveform of the PU to authentication the observed waveform. Beyond using just the communication waveforms, researchers [5] have suggested using additional cyclostationary signatures ("watermarks") that are built into the waveform to provide legitimate SU identification.

These solutions work only to authenticate if the malicious radio is not very clever or similar to the PUs. For instance, classification techniques do not work if the malicious radio waveform is in the same class as the PU waveform. Furthermore, most techniques can be fooled by simple replay style attacks. SDRs are very adept at replay attacks, having all the basic functionality of a Digital RF Memory (DRFM) device (a device that can receive RF transmissions and then play them back, varied in modulation, frequency, and time to fool and jam radar and communications radios). Combating replay attacks remains an open and challenging problem for authentication and non-repudiation. Some relief may come from actually demodulating the signal to digital and utilizing cryptographic authentication schemes. Other solutions may leverage the stochastic characteristics of the wireless medium that a replay attack would alter.

Besides needing to authenticate the users of spectrum, similar requirements exist for the underlying cognitive communication functionality. One area is the creation and distribution of objectives. CRs and CRNs make decisions to meet particular radio, network, and policy objectives. Integrity, authentication, and nonrepudiation are required to prevent the radios from receiving modified objectives or false objectives. [6] If false or modified objectives were given to all CRs, spectrum and other resources could be freed up for an adversary to use. If different objectives were given to different CRs, CR cooperative algorithms could break down and create adversarial behaviors.

CRs bring additional challenges to maintaining confidentiality. The wireless environment is more exposed physically than the wired environment, making all transmissions potentially receivable to all radios within range of the transmitter. Besides using encryption in applications and the network, frequency hopping and ultra-wideband (UWB) techniques can be used to provide varying degrees of confidentiality for the data. For a normal communications system, this is the main objective of confidentiality. However, because much of a CR system's functionality is dependent on the decisions it makes, providing confidentiality of the decisionmaking process also is needed. This may prove more difficult than data confidentiality. To begin with, CRs willingly share decisionmaking information with some subset of other CRs to create a more robust CRN. Even if these decisions are not shared explicitly, the actions on which the CR decides could be observed, giving insight into the decisionmaking process. In [7], a scheme is described in which a CJ jams a CR by repeatedly probing the CR with a false PU signal and then observing what frequencies the CR backs off to. By remembering the back off decisions, the CJ can determine the algorithm the CR is following and then use this knowledge to permanently jam the CR.

Although the commercial CRs of tomorrow will not be as open and flexible a platform as today's R&D CRs, they still will be considerably more flexible than a hardware radio. CRs and SDRs are attractive to manufacturers because they offer an ability to design hardware once and then write software to handle various use cases. For instance, a world handset could be designed with software written to handle various regulatory markets. Even if the system is "locked down" to a particular software build, any system running on a software platform has the potential to be compromised. Determining if the software has retained its integrity to operate correctly is a hard problem to solve.

Although actual approaches to compromising the integrity of a CR are varied, under a CRN configuration, malicious code has greater potential to propagate throughout the network. Even more worrisome, because of its "cognitive" capabilities, it might be possible for CR to become compromised without even modifying the actual codebase. Instead, the cognitive process of the CRs may be "taught" malicious behavior by malicious radios, which might also propagate throughout the network. This action would be analogous to children teaching each other bad manners at school. [8]

Once compromised, the flexibility of the compromised SDR platform gives it a large potential for mischief. Unlike hardware radios, in which the range of possible malicious activities is restricted by the functionality of the hardware, an SDR or a CR has the potential to be modified in software to perform new functionality; making the range of possible malicious activities the compromised radio can perform much larger. The potential capabilities of a hacked consumer-grade SDR to reduce overall medium availability for any wireless device in its frequency range will be much greater than the consumer grade hardware radios of the past.

Although these potential vulnerabilities and attacks may seem to indicate that cognitive communications will provide a host of new IA risks for wireless communication, several IA advantages exist. For instance, as a software-based approach, SDRs allow for the patching of vulnerabilities and updating of functionality. When bugs or flaws are identified in the software base, they can be corrected in ways that hardware radios cannot. Furthermore, the flexibility of using an A/D converter followed by a software-based approach may reduce the overall costs of radio designs by requiring fewer expensive RF components than a full hardware radio. R&D costs also should decrease because designs that work in simulation can be transferred almost directly into implementation. All this means that barriers to entry will be reduced, which in conjunction with DSA, will allow spectrum to be more efficiently used.

The cognitive and adaptive capabilities of CRs and CRNs may also provide IA advantages. The decisionmaking processes could be used to discern malicious radio behavior from normal behavior. In a CRN, transmissions could be adapted around the malicious radios to alleviate availability issues and provide additional confidentiality. A robust trust architecture, necessary for authentication, integrity, and nonrepudiation also can be strengthened by the cognitive process. As stated in, [9] combining the cognitive capabilities with IA functionality will allow the CRs and CRNs to "exhibit good judgment," a capability normally associated with a human rather than a machine.

The coming transition to cognitive communication devices will have a significant impact on the communications landscape. The DSA application alone has the potential to upend the foundations of wireless spectrum access. Unfortunately, these devices will have positive and negative implications to the IA objectives of availability, authentication, integrity, nonrepudiation, and confidentiality. History has taught us that identifying these issues early is the best vaccine against future IA problems. ■

References

1. J. Mitola, Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio. PhD thesis, Royal Institute of Technology (KTH), 2000.
2. R. W. Thomas, L. A. DaSilva, and A. B. Mackenzie, Cognitive networks, in Proc. of IEEE DySPAN 2005, pp. 352-360, November 2005.
3. S. Haykin, Cognitive radio: Brain-empowered wireless communication, IEEE Journal on Selected Areas in Communication, vol. 23, pp. 201-220, February 2005.
4. A. Sethi and T. X. Brown, Hammer model threat assessment of cognitive radio denial of service attacks, in Proc. of IEEE DySPAN 2008, 2008.
5. P. D. Sutton, K. E. Nolan, L. E. Doyle, Cyclostationary signatures for rendezvous in OFDM-based dynamic spectrum access networks, in Proc. of IEEE DySPAN 2007, pp. 220-231, 2007.
6. Y. Zhang, G. Xu, and X. Geng, Security threats in cognitive radio networks, in Proc. of HPCC 2008, pp. 1036-1041, Sept. 2008.
7. L. Ma and C.-C . Shen, Security-enhanced virtual channel rendezvous algorithm for dynamic spectrum access wireless networks, in Proc. of IEEE DySPAN 2008, 2008.
8. T. Clancy and N. Goergen, Security in cognitive radio networks: Threats and mitigation, in Proc. of IEEE CROWNCOM 2008, pp. 18, May 2008.
9. J. Burbank, Security in cognitive radio networks: The required evolution in approaches to wireless network security, in Proc. of IEEE CROWNCOM 2008, pp. 17, May 2008.

About the Authors

Capt Ryan Thomas | is an Assistant Professor of Computer Engineering at the Air Force Institute of Technology. Capt Thomas received a BS in Engineering from Harvey Mudd College, an MS in Computer Engineering from the Air Force Institute of Technology, and a PhD from Virginia Polytechnic Institute and State University, Blacksburg, VA. His research interests include computer networking and wireless communications systems. Special interests include cognitive networks, autonomous distributed decisionmaking, wireless network topology control and modeling of networking problems using game theory.

Lt Col Brett Borghetti | is an Assistant Professor of Computer Science at the Air Force Institute of Technology. Lt Col Borghetti received a BS in Electrical Engineering from Worcester Polytechnic Institute, an MS in Computer Systems from the Air Force Institute of Technology, and a PhD in Computer Science from the University of Minnesota. His research interests include opponent modeling, metareasoning, artificial intelligence, machine learning, information theory, and game theory.

▷ *continued from page 11*

SUBJECT MATTER EXPERT

economies. In the Security Economics session, Dr. Acquisti presented results from various experiments that show the importance of contextual factors for willingness to divulge personal data and willingness to adopt security measures. The research raises questions about individuals' capacity to make optimal disclosure and security decisions in complex information environments.

Dr. James Hoe is an Associate Professor of Electrical and Computer Engineering. His research interests are in computer architecture and high-level hardware description and synthesis. Dr. Hoe presented the Behavior-based Email Filtering System (BEEFS) in the Trustworthy Computing session. BEEFS facilitates the delivery of malware-free emails by integrating with the mail server or acting as a mail proxy. BEEFS monitors the execution of email attachments in a clean virtual machine (VM) and identifies suspect executables by looking for automatically learned behavioral signatures. In the current BEEFS prototype, the malware detector recognizes malware behaviors by simple patterns in the sequence of system calls and the associated arguments. These behaviors can be extracted automatically by training against known malware and later be used to identify suspicious activities of unknown executables.

Dr. Jason Hong is an Assistant Professor in Computer Science. His current research areas include ubiquitous computing and usable privacy and security, focusing on location-based services, anti-phishing, mobile social computing, and end-user programming. In the Protecting Privacy and Confidentiality of Information session, Dr. Hong presented an overview of the Supporting Trust Decisions project. This project focuses on developing better user interfaces to help people make better trust decisions, developing mechanisms to teach people not to fall for phishing attacks, and better machine learning and information retrieval algorithms that can automatically detect phishing attacks. ■

"Enabling," Web 3.0

by Daniel Shorey

The World Wide Web has evolved from its humble beginnings as Web 1.0, or simple Web pages that link to other simple Web pages, into today's more advanced Web 2.0, which consists of complex pages that promote applications and information, both personal and proprietary, in vast warehouses of data.

Moving forward, Web 3.0 is poised to take advantage of new design principles and collaboration through a variety of enabling technologies. Some of these new technologies and concepts are already beginning to take root.

Think of the Web as a cloud of information with little to no organization differentiating the volumes of available knowledge. Information exists but computers have no way of differentiating one piece of data from another. For all of the advances of Web 2.0 you still must access this information through keywords, sifting through thousands of potential results until you find one that matches your requirements.

As the Web advances, connecting data objects and pages is not enough. Web 3.0 is about creating technology that interacts and functions in the same way we do with the world around us. Put simply, artificial intelligence, or intelligence that can turn the current information into data that can be understood and evaluated on its own by computers. The Web will become smart and there will be distinction based upon meaning.

This newest generation of Web should be considered a "mash-up" of applications driving towards a "Smart Web." Currently, in the earliest stages of transition from 2.0 to 3.0, many of the tools are considered crude, like Facebook and social media sites, but crucial in reaching the ultimate goal of a functional interactive world-aware Web. Essentially, the Internet or Web-enabled device would "understand" the input of information providing a more fluid and intuitive experience to the user.

Pressures from companies like Flickr and Google, which are working to develop and push intelligent Cloud applications, are forcing traditional models to rethink and reorganize their software development to meet the changing expectations of new generations that have to expect instant gratification.

Removing the informational walls between applications is at the very core of Web 3.0. Companies, like Microsoft, that have thrived and relied on the single license model, are beginning to tear down the walls of their applications in response to the movement to Web 3.0. For instance, Microsoft is making their future applications, the next generation of Office and some current Office features, available online in the "Cloud" without the need for source software in the licensing model.

Web 3.0 will take advantage of the growth in computer power and general bandwidth, becoming a singular platform that delivers a single intelligent quasi-human interface experience. There is growing debate about the driving force behind Web 3.0—will the driving force be intelligent systems, or will intelligence emerge in a more organic fashion, *e.g.* a collaborative filtering that extracts meaning and order from the existing Web and shapes how individuals interact with it. It matters little how it develops as long as it meets the end goal of intelligent data interpretation.

Web 3.0 can also be considered as a shift towards 3-dimensional presentation. This would require the Web to transform into 3D spaces, taking collaboration further through the use of shared 3D spaces.

At the Seoul Digital Forum, Eric Schmidt, CEO of Google, was asked to define Web 2.0 and Web 3.0.

"Web 2.0 is a marketing term, I think you have just invented Web 3.0. But if I were to guess what Web 3.0 is, I would tell you that it is a different way of building applications… My prediction is that Web 3.0 will ultimately be seen as pieced together applications that are pieced together. There are a number of characteristics—The applications are relatively small; the data is in the cloud; the applications can run on any device, PC or mobile phone; the applications are very fast and they are very customizable. Furthermore, the applications are distributed virally, literally by social network, by email. You won't go to the store

▷▷ continued on page 30

A Statechart Model of the Cross Domain Implementation Process

by CDR Michael Schumann

Disclaimer

The views expressed in this article are those of the authors and do not reflect the official policy or position of the US Department of the Navy, Department of Defense, or the US Government.

The charter of the Unified Cross Domain Management Office (UCDMO) is to address the needs of the Department of Defense (DoD) and the intelligence community (IC) to share information and bridge disparate networks. [1] The UCDMO has several concurrent initiatives designed to align and federate the implementation and support of cross domain solutions (CDS). The UCDMO recently published the following guidance materials on cross domain (CD) implementations of information systems—CD Community Roadmap, CD Inventory List, and CD Implementation Process (CDIP), all of which are available at *http://www.intelink.gov/sites/UCDMO*.

Our research focuses on applying formal methods-based tools and techniques to the largely human-based CDIP (see Figure 1). As Monin points out in [3], formal methods provide us with a precise and unambiguous means of specifying and reasoning about the behavior of systems. Formal methods are most frequently used in the software engineering of security—and safety—critical systems. However, this research demonstrates the use of formal methods to specify and reason about the process used to implement cross domain solutions. The intent of our approach is to impart a high degree of precision to our understanding of the process, as well as to provide an automated means of validating that the process does all and only what we expect it to do. In this article we will discuss our methodology as well as the formal methods tools and techniques that we use to model the process.

Needs and Challenges

Encompassed within the CDIP is the Intelligence Community Directive 503 (ICD 503) certification and accreditation (C & A) process. [4] This process is the means by which the designated authorities such as the Cross Domain Resolution Board (CDRB) decide whether to allow a given CDS to operate. The UCDMO is not a decision making body; rather, they are responsible for the development, coordination, and oversight of the CDIP. We view the CDIP as critical to building the evidence necessary for decision makers to weigh the risks of operating a given CDS and to make the accreditation decision for the system.

The CDIP is designed as a process that is easy for humans to understand and follow. Historically, the field of formal methods was born out of a need to rigorously specify and verify hardware

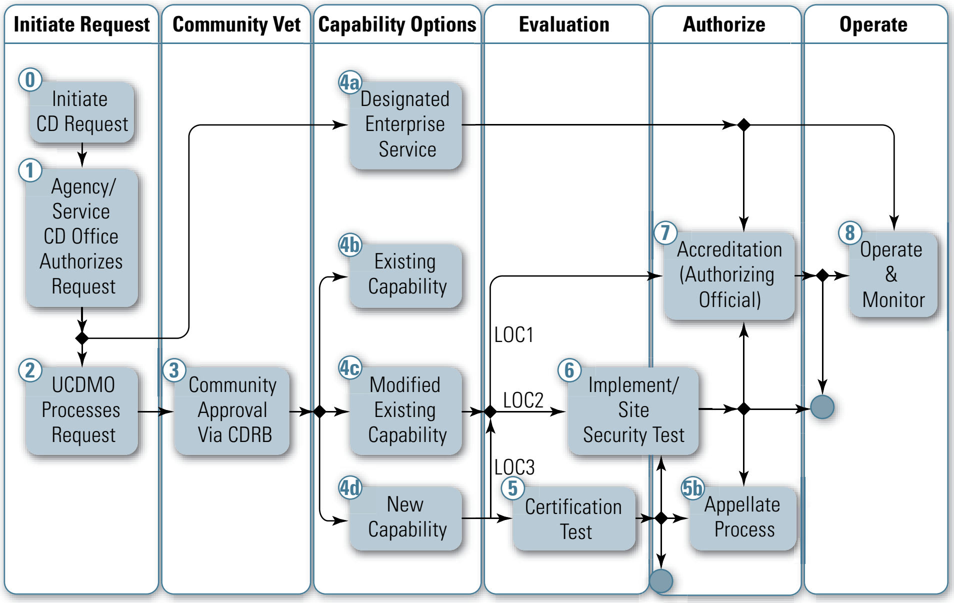


Figure 1 Cross Domain Implementation Process [2]

and software systems, especially in the case of security—and safety—critical systems. [3] Therefore, formal methods tools and techniques are typically based on well-established mathematical theories. One of the challenges of formally modeling a process designed for humans is capturing those portions of the process that involve subjective human activities like evaluation and decision making. For example, Step 1 of the CDIP demonstrates the subjective nature of the process. In this step, a newly initiated cross domain request form (CDRF) must be validated and authorized by the requestor's agency/service CD office, a very human-centric activity. Such activities need to be formally specified within the context of the process. In the next section we discuss our approach to accomplish this. We evaluated several computer-based tools to support our method of formally specifying the CDIP. For instance, Communicating Sequential Processes (CSP) [5] provides for specifying systems of parallel agents that communicate by passing messages between them. [6] However, like many formal methods, CSP is based on a relatively complex mathematical notation which represents an entry barrier to the casual reader. Ryan and Schneider present a simple example of a CSP sentence that captures the notion of a choice between the actions of two processes and then behaves like the one chosen—

$$\boxed{?x: A \rightarrow P(x) = (?x : B \rightarrow P(x)) \square (?x : C \rightarrow P(x))}$$

For a detailed treatment of this and other CSP examples, refer to. [6] We merely wish to point out that formal methods often require the use of complex mathematical notation which can be difficult to learn and use effectively.

In order to avoid the representation complexities associated with formal notations like that of CSP, we represent the CDIP using a statechart-based approach, By using this approach we effectively lower the entry barrier by presenting complex formal models in a notation that is visual in nature and relatively easy to learn and understand. As a result, we expect this formal modeling approach to be palatable to a wide community of users versus the relatively small community involved in applying computer-assisted formal methods today.

Statechart Based Formal Modeling

Harel introduced the concept of statecharts in [7] and Drusinsky applies Unified Modeling Language (UML) statecharts to real-world specification and verification in. [8-10] In addition, Drusinsky has developed a user-friendly statechart modeling plug-in called StateRover for the Eclipse integrated development environment (IDE). [8] This tool allows the user to generate complex statechart models with multiple layers of abstraction and perform automatic syntactic validation of the model. In addition, the tool auto-generates executable C, C++, or Java code from the model. Figure 2 demonstrates a simple traffic light controller (TLC) model designed with the StateRover modeling tool. Figure 3, a detailed view of *CoarseState_Red* shown in Figure 2, demonstrates the ability to represent levels of abstraction (referred to as hierarchy or state nesting) with

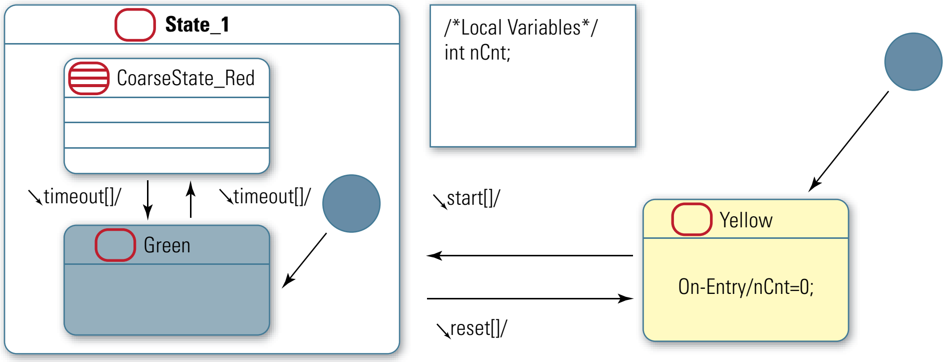
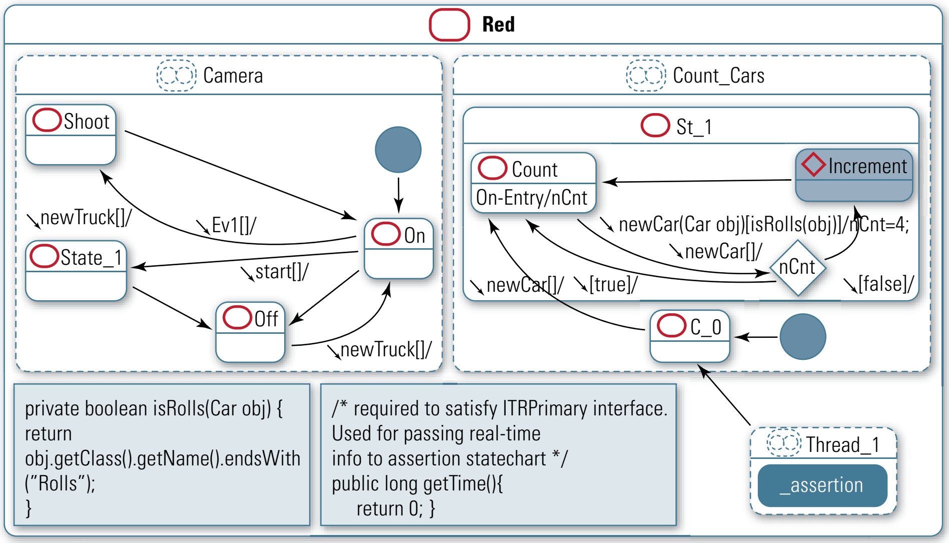


Figure 2 Statechart Model of Traffic Light Controller



```
private boolean isRolls(Car obj) {
return
obj.getClass().getName().endsWith
("Rolls");
}
```

```
/* required to satisfy ITRPrimary interface.
Used for passing real-time
info to assertion statechart */
public long getTime(){
    return 0; }
```

Figure 3 Detail View of CoarseState_Red

StateRover. Figure 3 also represents the use of embedded assertions (the box labeled *Thread_1*) that ensure that the model adheres to requirements specified in a separate statechart. This provides a flexible and reusable method of ensuring that the model's behavior conforms to requirements. The TLC example is derived from. [8]

The code generation module performs a series of syntactic checks on our model ensuring that the model conforms to the underlying, well-defined set of rules (syntax) for statecharts. In the next section we discuss code generation in the context of our model of the CDIP.

Cross Domain Implementation Process Model

StateRover was designed to facilitate the design of software for complex reactive systems. We are using this tool in a novel way to model the human-based CDIP as shown in Figure 4. By doing so, we are able to take advantage of automated statechart handling capabilities built into StateRover such as hierarchy, concurrency, syntactic validation, and automated testing. Hierarchy allows us to nest states, as previously shown in the TLC example, in order to build multiple layers of abstraction for our model. This effectively allows us to "zoom" in or out to view the model at higher or lower levels of detail, respectively.

Statechart concurrency allows us to capture the notion of fully or partially independent activities occurring at the same the time. Figure 5 demonstrates the use of concurrency showing the partially independent activities that occur in Step 5 of the CDIP. The box labeled *CT_and_E shows* the decision process that occurs during Certification Test and Evaluation (CT&E), while the box labeled *Add_to_Baseline* shows the concurrent decision process to add a system to the UCDMO's CD Baseline. In practice, as soon as a system passes CT&E it moves on to Step 6 (Implementation). At the same time, the system is evaluated by the UCDMO for possible addition to the CD Baseline list. We are able to capture these concurrent and partially dependent activities with the state concurrency (the blue box in Figure 5 connecting *CT_and_E and Add_to_Baseline*) feature of StateRover.

Assertions as Requirements

In the formal methods domain, we typically wish to ensure that our formal models adhere to a set of stated requirements. Statecharts do this through the use of embedded assertions which act as requirements. *The Thread_1* box of Figure 3 is an example of an assertion statechart embedded within another

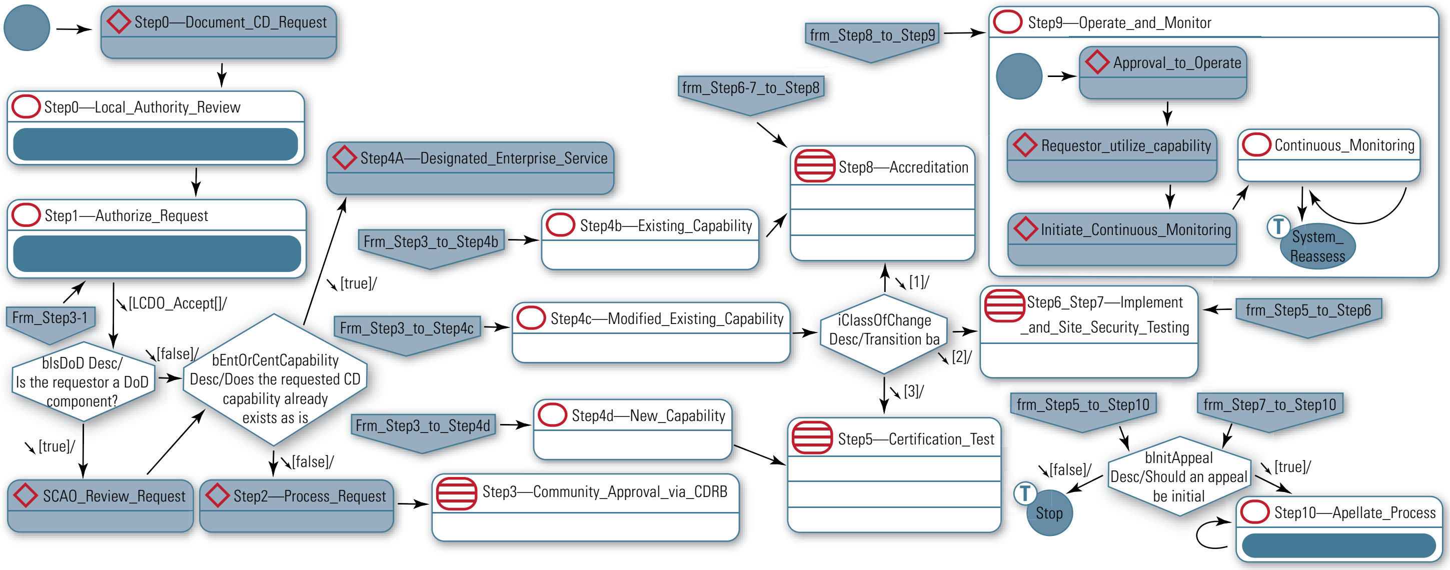


Figure 4 Statechart Based Formal Model of the Cross Domain Implementation Process

statechart, called the primary. Figure 6 shows the full version of the assertion statechart. During testing, which we will discuss in the next section, failures to adhere to the requirements of the assertion are recorded and reported by the testing module. The aim here is to validate that our model behaves as we expect under a wide variety of conditions.

Code Generation and Testing

StateRover's automated code generation module provides a means of both syntactically checking our model and creating and using automated testing scenarios to validate the performance of our model under specific conditions. As the user builds a statechart diagram, StateRover builds a corresponding XML file that exactly describes the diagram. StateRover enforces a well-defined, formal set of rules governing the structure (*i.e.* syntax) of relationships described in this XML document. The code-generation module rigorously validates the model for compliance with these rules and provides the user with visual and textual indicators of errors discovered in the process. This allows the user to quickly discover and correct errors in his model such as undefined variables, missing references to other levels of the model, or missing transitions between elements of the model. Successful code generation provides us with an "executable" version of our model in one of three user-selectable programming languages; C, C++, or Java. It is important to note that our research is not focused on designing software per se; instead we are taking advantage of the code generator's built-in functionality to perform validation and testing of our model. The JUnit-based testing module works in conjunction with StateRover's animation server to visually and textually inform the user of testing progress and final results. For example, Figure 7 shows Step 3 of the CDIP model just after a test run. Colored boxes represent those elements or states that were visited during the test run.

The research discussed in this document is ongoing; however, the preliminary results from applying our approach indicate that statecharts and the associated tools can be applied in an effective manner to model and validate human-based processes. After accomplishing the steps discussed above to build and remove errors from the model of the CDIP, we successfully generated code and were able to run tests against that code. The results of the first test run demonstrated that under the test conditions provided to the model we were unable to progress past Step 3 during the test run. The result provided immediate feedback on a problem with the model which we were able to quickly troubleshoot and address due to the visual and textual feedback mechanisms of the tools. We have not applied embedded assertions to the CDIP model; however, we see this as the next logical step.

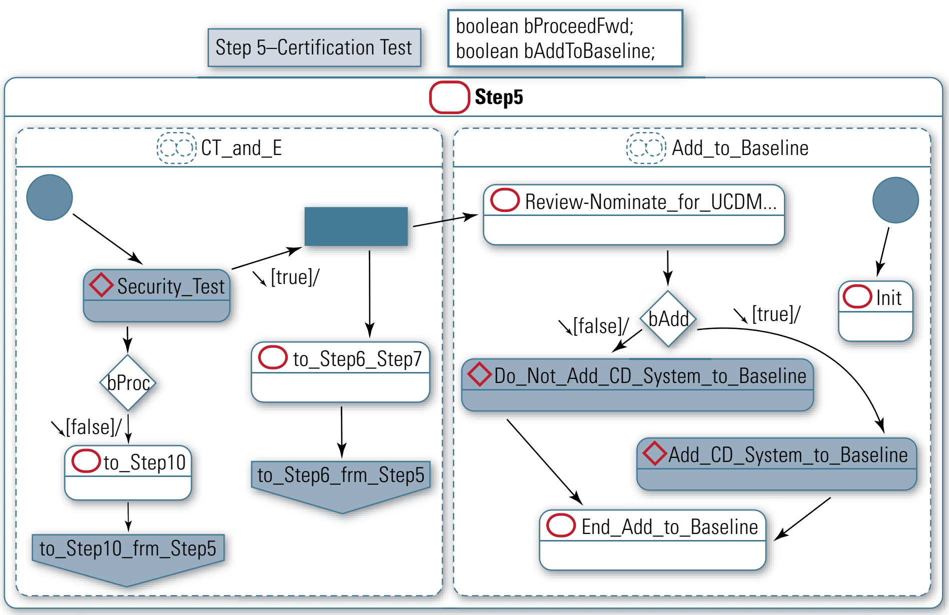


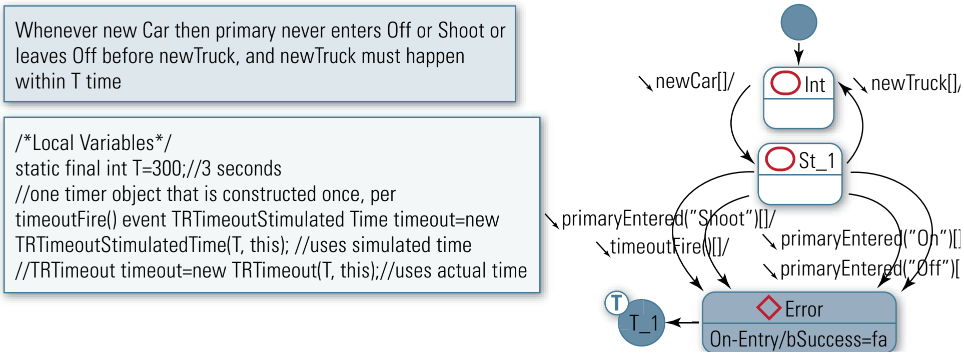
Figure 5 Certification Testing Assertions as Requirements

Future Work

Plans for ongoing research will include the application of embedded assertions to the model as a means of enforcing requirements on the process. Future research will also include a demonstration that this approach to formal process modeling provides a better way to do requirements engineering—by capturing assertions while building the model and subsequently turning those assertions into requirements.

Conclusion

Computer-assisted formal methods provide us with a way to precisely develop, model, and validate human-based processes. Preliminary investigations indicate that our work in this area will ultimately benefit the cross domain community by providing a



Whenever new Car then primary never enters Off or Shoot or leaves Off before newTruck, and newTruck must happen within T time

```
/*Local Variables*/
static final int T=300;//3 seconds
//one timer object that is constructed once, per
timeoutFire() event TRTimeoutStimulated Time timeout=new
TRTimeoutStimulatedTime(T, this); //uses simulated time
//TRTimeout timeout=new TRTimeout(T, this);//uses actual time
```

Figure 6 Example of Assertion Statechart

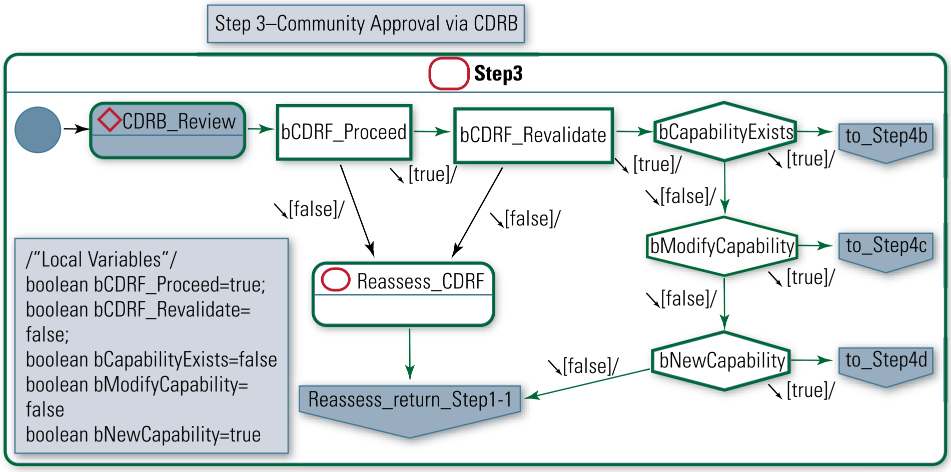


Figure 7 Step 3 Post Testing

rigorously validated and very precise process for the implementation, certification and accreditation of cross domain solutions. In addition, our proposed approach can be generalized to other processes, particularly those in safety—and security—critical domains. ■

References

1. M. Bailey. (2008, July). The unified cross domain management office: Bridging security domains and cultures. Crosstalk Magazine 21(7), pp. 21-23.
2. UCDMO, "CD Implementation Process," August. 2008.
3. J. Monin, Understanding Formal Methods. Springer, 2003, pp. 276.
4. Director of National Intelligence. (2008, September 15). Intelligence community directive number 503: Information and information systems governance. [Online]. Available: *https://www.intelink.gov/mypage/c&a.*
5. Hoare, C. A. R., Communicating Sequential Processes. Englewood Cliffs, N.J. : Prentice/Hall International, c1985., 1985, pp. 256.
6. P. Y. A. Ryan, S. A. Schneider, M. H. Goldsmith, G. Lowe and A. W. Roscoe, Modelling and Analysis of Security Protocols. ,1st ed.Addison-Wesley Professional, 2000, pp. 320.
7. D. Harel, "Statecharts: A visual formalism for complex systems," Sci. Comput. Program., vol. 8, pp. 231-274, 1987.
8. D. Drusinsky, Modeling and Verification using UML Statecharts: A Working Guide to Reactive System Design, Runtime Monitoring and Execution-Based Model Checking. Newnes, 2006, pp. 400.
9. D. Drusinsky, J. B. Michael, T. W. Otani and M. Shing, "Validating UML Statechart-Based Assertions Libraries for Improved Reliability and Assurance," Secure System Integration and Reliability Improvement, 2008. SSIRI '08. Second International Conference on, pp. 47-51, 2008.
10. D. Drusinsky, M. -. Shing and K. A. Demir, "Creation and Validation of Embedded Assertion Statecharts," Rapid System Prototyping, 2006. Seventeenth IEEE International Workshop on, pp. 17-23, 2006.

About the Author

CDR Michael Schumann | is a Navy Commander and doctoral student in the Software Engineering program at the Naval Postgraduate School. His dissertation supervisor is Professor Bret Michael of the Department of Computer Science. He may be reached at *maschuma@nps.edu.*

▷ *continued from page 25*

"ENABLING," WEB 3.0

and purchase them… That is a very different application model than we have ever seen in computing."

—Eric Schmidt, May 2007

In many cases, the application of Web 3.0 will denote the graduation to continued performance across platforms, increased artificial intelligence and information handling, sustained bandwidth speeds and a more cloud-centric model of application usage and distribution.

Only one question remains, how long will it take for these ideas to become a stable, reliable, and intuitive reality? ■

About the Author

Daniel Shorey | has been in the information technology and web-development field for 15 years. Currently working in support of multiple government clients, Mr. Shorey plans, develops, and implements client portals, custom web applications and general design work. He may be reached at *iatac@dtic.mil.*

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
□ The Insider Threat to Information Systems

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	□ No. 4
Volumes 11	□ No. 1	□ No. 2	□ No. 3	□ No. 4
Volumes 12	□ No. 1			

Fax completed form to IATAC at 703/984-0773

Calendar

May

SANS Security East 2009
4–12 May 2009
New Orleans, LA
https://www.sans.org/securityeast09/index.php

Electronic Warfare Fundamentals and Planning Course
11–15 May 2009
Alexandria, VA

30th IEEE Symposium on Security & Privacy
17–20 May 2009
Oakland, CA
http://oakland09.cs.virginia.edu

June

Information Assurance Collaboration Forum
2 June 2009
Laurel, MD
https://www.disa.mil/conferences/index.html

DoD Enterprise Architecture
1–4 June 2009
St. Louis, MO
https://www.afei.org/brochure/9a05/index.cfm

Red Team/Blue Team Symposium
2–5 June 2009
Laurel, MD
https://www.nsa.gov/ia/events/

July

22nd IEEE Computer Security Foundations Symposium
8–10 July 2009
Port Jefferson, NY
http://www.cs.sunysb.edu/csf09/

Black Hat USA 2009 Briefings and Trainings
25–30 July 2009
Las Vegas, NV
https://www.blackhat.com/

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

IATAC

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