11/3

Volume 11 Number 3 • **Fall 2008**

IAnewsletter

The Newsletter for Information Assurance Technology Professionals

Guarding the Cybercastle in 2020

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 Director:	Christina P. McNemar
Creative Director:	Ahnie Jenkins
Art Director:	Don Rowe
Copy Editors:	Gina Abruzzese Louise Price
Designers:	Ricardo Real Dustin Hurt Kacy Cummings Ted Pringphayune
Editorial Board:	Ronald Ritchey Tara Bissett Gene Tyler Angela Orebaugh

***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
Winter 2008 October 31st, 2008

Cover design: Ricardo Real
Newsletter design: Donald Rowe

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

feature

in every issue

IATAC Chat

Gene Tyler. IATAC Director

The free 4-hour technical inquiry service is a basic research service offered to our IATAC customers. This service is available to all Department of Defense (DoD) and government personnel as well as Defense Technical Information Center (DTIC) registered users.

In issues past, I've discussed some of the remarkable free products we offer to customers of the Information Assurance Technology Analysis Center (IATAC), such as State-of-the-Art-Reports (SOAR), various Tools Reports, the IA Digest, the Research Update, of course our award-winning *IAnewsletter*, and many, many more. However, I have yet to really cover the additional free services and resources we offer, including our Subject Matter Expert (SME) Program and our 4-hour technical inquiry service—services that actually go hand in hand.

The free 4-hour technical inquiry service is a basic research service offered to our IATAC customers. This service is available to all Department of Defense (DoD) and government personnel as well as Defense Technical Information Center (DTIC) registered users. As part of IATAC's mission objectives, we prepare and disseminate technical inquires or anticipated technical inquires from our users. Users request technical inquires via email, by phone, in person, or through our website. These inquiries cover the spectrum of basic strategy, policy, and governance to enabling technologies, system development, analysis, operations, and support. In addition, we maintain a detailed record of all inquires for future reuse by other customers looking for the same or similar information. For information on our technical inquiry program, please visit our website at *http://iac.dtic.mil/iatac/inquires.html.*

Although IATAC has a robust in-house network of experts, the broad nature of IA makes it impossible for us to cover all possible areas in the field. For this reason, we have developed our SME Program. The SME Program is a completely voluntary effort comprising Information Assurance (IA) professionals from areas such as the government, industry, and academia. IATAC primarily uses these experts to assist in responding to technical inquiries—hence how the two services go hand in hand. We also rely on the SMEs to share scientific and technical information that may have a significant impact on the entire IA community (articles, technical papers, research, *etc.*).

Through the program, SMEs have the opportunity to share their extensive IA knowledge with other IA professionals throughout the community; in fact, they often author many of the articles you read quarterly in this publication. IATAC receives more than 200 IA-related technical inquiries per year from DoD and the Government. SMEs are a pivotal resource for the IATAC mission. Often, they provide valuable information that IATAC passes on to requestors. SMEs also serve as direct points of contact whom the requestor may reach out to for further details regarding a specific inquiry.

In addition to supporting our inquiry service, SMEs are valuable contributors to our Scientific and Technical Information (STI) library. To support the advancement of science and technology, the DTIC has chartered IATAC (DoD Instruction 3200.14, 13 May 1997, and DoD Directive 3200.12, 11 February 1998) to collect STI, which includes technical papers, electronic data, audio, photographs, video, briefings, *etc.* The continuous flow of STI from SMEs to the IATAC STI collection continues to have a significant and successful impact on the IA community. For more information on our SME Program, please visit our website at *http://iac.dtic.mil/iatac/sme.html.*

In this edition of the *IAnewsletter* you will, once again, find several articles of interest written by experts throughout the field. In the meantime, if you have any questions or concerns regarding the inquiry process, the SME Program, or other parts of IATAC, please do not hesitate to email us directly at *iatac@dtic.mil.* ■

Gene Tyler

FEATURE STORY

Guarding the Cybercastle in 2020

by Todd McDonald, Bert Peterson, Dan Karrels, Todd Andel, and Rick Raines

Abstract

Monitoring and defending current and future US Air Force (USAF) networks will require a synergy of emerging technologies and some degree of novelty in both acquisition and operational art. In this article, we examine possibilities for future distributed defensive architectures and consider them in light of security and trust. As we consider current research efforts devoted to information and network security, we catch a brief glimpse at what the future cyber defense landscape, or "Cybercastle," may look like.

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 US Government.

Introduction

Many of the commercial systems found in the developed and developing world depend on computers and communication networks for the ability to conduct enterprise activities. Similarly, the Department of Defense (DoD) has overlaid major operational capabilities on information networks that support command, control, and communications (C3) at various levels. In 2005, the USAF officially recognized the criticality of the information domain as a strategic warfighting resource and redefined its mission statement to include "deliver sovereign options for the defense of the United States of America and its global interests—to fly and fight in Air, Space, and Cyberspace". [1] Secretary of the Air Force Michael W. Wynne subsequently reinforced this vision with the creation of a Cyberspace Command (AFCYBER). [2] The DoD has recently refocused its formal definition of cyber as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers," consistent with presidential cyber security policy. [3] In any current military understanding, cyber defense squarely encompasses computers (embedded and standalone) and their interconnectivity.

Currently, we are seeing a flood of threats to the electronic infrastructure of governments around the world, including our own. As we consider the landscape of the USAF network infrastructure over the next decade, we may also consider possibilities for defending that infrastructure in a holistic, secure, and trusted manner. It makes sense as well that whatever revolutionary changes we may ultimately consider, the entire panorama of the defense industrial base (DIB) and our national commercial interests are envisioned. The Cybercastle, in this view, encompasses (but is not limited to) portions of the Internet that support military and high-encryption systems, DoD intranets, external information systems, wireless/radio communications systems, and infrastructure control systems using Supervisory Control and Data Acquisition (SCADA) systems.

Today, nearly 10% of all Internet nodes belong (unknowingly) to a malicious multi-agent system whose owner waits for a high bidder to make use of its services. As Internet usage worldwide continues to grow, and with average users unaware of their vulnerability to assimilation into a malicious C3 network, the next decade promises huge challenges directly rooted in cyber-network defense and protection. To deal with the possibilities for cyberterrorism in the ongoing Global War on Terrorism (GWOT) or possible malicious attacks of nation-state actors against the Cybercastle, we turn our attention to high-level goals for building defensive systems. What will the castle look like a decade from now? How strong will its walls be, or how strong do we *need* the walls to be in light of the veracity of those on the other side of the moat? What is a wall or a moat in cyberspace, given that threats can also come from inside the network? We discuss thoughts on these topics and give some insight on what technological advances or prices will most likely be paid to ensure the Cybercastle's resilience.

Currently, we are seeing a flood of threats to the electronic infrastructure of governments around the world, including our own. As we consider the landscape of the USAF network infrastructure over the next decade, we may also consider possibilities for defending that infrastructure in a holistic, secure, and trusted manner.

Defensive Cyber Platforms

In the domain of space and air, the USAF focuses strategic and operational capabilities across a range of platforms, where we define a platform as a delivery vehicle for some suite of weapons (bullets from a Gatling gun, air-launched cruise missiles, air-to-air missiles, *etc.*) that support some set of missions and objectives (suppression of enemy air defense, close air support, air superiority, *etc.*). In some cases, the platform itself provides the actual strategic advantage; in other cases, the weapons (or payloads) delivered by the platform are of greater significance. Platforms, in general, exhibit long service life, incur large capital investment, support a variety of missions (consider the evolution of the B-52 bomber), and undergo intense scrutiny to guarantee reliability or operational qualities. Payloads, on the contrary, emerge from rapid development lifecycles and achieve specific effects in some tactical, operational, or strategic context.

Targeting cyber as an operational domain will produce a wide variety of cyber platform and payload manifestations over the next decade. Though cyber as a warfighting domain is not limited to information networks and their underlying capabilities, we abuse the term slightly so we may consider platforms that might support holistic network defense capabilities. In considering defensive cyber platforms, we use the term "Cybercraft" to embody the notion of a delivery platform for C3 defensive capabilities. In our technical paper we posed the first conceptual use of Cybercraft as an autonomous, intelligent agent that accomplishes military purposes across a wide variety of electronic-based media. [4] The Air Force Research Laboratory (AFRL) Information Directorate has continued the vision with a project aimed at furthering basic research areas that support platform and payload integration for defensive missions.

As AFRL's research partner in this endeavor, the Air Force Institute of Technology (AFIT) is considering a broad range of development possibilities for future defensive cyber platforms and is supporting technologies for the Cybercraft project itself. While keeping one eye on the needs of current USAF network defenders and keeping the other eye on the horizon to see what the art of the possible may be, we consider what the platforms used to defend the Cybercastle in the future may look like.

Building the Cybercastle

The defense of USAF networks in the future must not rely on the notion that a Maginot line exists that is beyond penetration. As history clearly reveals, the ways around a wall are more numerous than one might assume. It is common knowledge that enemies exist almost as abundantly within walls as they do outside of walls. For example, the Computer Emergency Response Team (CERT) Coordination Center found that the vast majority of the government insider incidents (90%) were caused by current employees, and most (58%) were people in administrative positions requiring limited technical skill. [5] Despite proof of security or empirical demonstration of our finest defensive tools, acts prompted from social networking attacks that are foisted on non-malicious insiders can void the best technical layers of defense.

The defensive cyber platforms of the future must have several qualities that will provide them freedom to maneuver and operational resilience in the face of such adversarial waters, whether the attempts to compromise mission activities come from inside or outside the network infrastructure. We envision platforms with the ability to execute a wide variety of generic capabilities using a common, payload-based framework. Until we find a more appealing future abstraction, distributed multi-agent systems (DMAS) is a close picture for what this defensive architecture could look like: compositions of light- to heavy-weight agent components that securely communicate, collaborate, and respond to cyber attacks of a wide variety. Because this cyber DMAS will defend existing and future military C3 systems, we have additional constraints that typical commercial networks may not be concerned with. Namely, cyber platforms must operate under tighter security, ensure fault tolerance and self-healing, and ultimately affect human life in some way (*i.e.,* failing to protect critical mission systems).

Figure 1 depicts, in standard Unified Modeling Language (UML) format, a conceptual domain model of interest to consider future defensive architectures. At a basic level, *platforms* serve to protect specific *host* nodes with a network or IP-based context (desktop machines, routers, hand-held devices, radio equipment, *etc.*). At a basic level, platforms possess *state* and execute *payloads* of various kinds: *sensors*, *behaviors*, and *effectors,* just to name a few. Payloads provide the touch point to the *environment*, which we define as the collective space of hosts connected to hosts *via networks* where hosts are controlled by some *OS* that runs *applications*. Payloads gather data about environmental components or alter the environment through specific effects. We define information about the environment and the conceptual glue that binds platforms and payloads to hierarchical levels of command and control as state, and we use behavior payloads to describe decisionmaking engines that bring logical correlation with sensor conclusions. We note that platforms share some state in a global context when payloads need to collaborate and keep other's knowledge local when payloads need only host-based context.

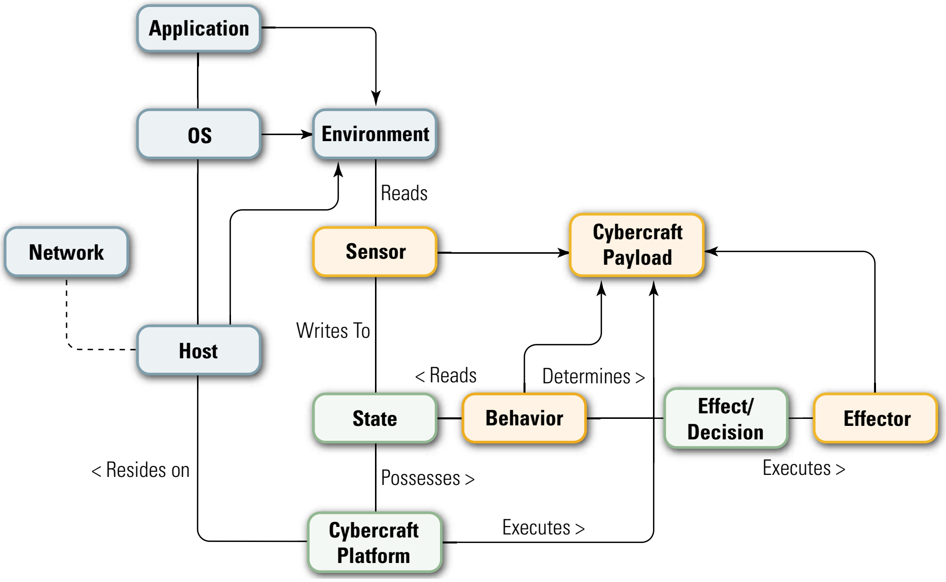


Figure 1 Conceptual Defensive Cyber-Network Domain Model

Much of the basic technology and defensive tools for our next-generation architecture exists in some form today, whether in commercial products or academic prototypes, and many research areas already give us considerations for platform design choices or specific payload configuration. Because basic functionalities—such as virus checkers, trust frameworks, trusted hardware components, self-repairing application environments, host-based integrity checkers, malware detection suites, and intrusion detection systems—all exist in some form currently (many immature but nonetheless demonstrable), one important question remains: what would a future defensive cyber platform most need so that we may rapidly, reliably, and securely integrate these technologies over time? In other words, what is the true revolutionary idea that our future defensive systems will need that our current tool suites do not provide?

We begin to answer these questions by considering that any single available technology is currently limited when used alone or used in a defensive vacuum. Namely, how do we measure the strength of any given technique when faced with an adversary that has subverted the OS or has taken control of the network infrastructure at some fundamental, administrator-privileged level? We can visualize this conundrum further by considering a modern virus checker that defends a system correctly as long as its signature-based algorithms detect and prevent *known* software threats from running maliciously. Unfortunately, "we do not know what we do not know," and this reflects more poignantly in our signature-based defensive mechanisms. In addition, these naive systems fail without having the full context of an attack. If the attack is "low and slow" or highly distributed and dynamic, we should focus on the context of the attack, not the manifestation of it.

Assuming an adversary does not successfully install an administration-level root kit with power to alter kernel-level operations and assuming we have a correct and current signature set to evaluate possible threats, a virus checker may provide defense along discrete attack vectors. Unfortunately, we cannot guarantee any of our base assumptions with any consistent measure. All application-level, virtual-level, and OS-level defensive techniques share this common weakness: they can be lied to by any of the underlying hardware components of a system or by the operating system that manages those components if an adversary gains root-level host access. As Figure 1 depicts, the notable difference of future cyber defensive platforms should be their independence from the rest of the environment in which they protect and operate. This concept depicts the only reliable way around a possible cycle of deception. We liken this concept to the military notion of taking the "high ground," and we call this cyber high ground the *root of trust*, which forms our number one priority in building the walls of the future Cybercastle.

Secure Root of Trust

Secure root of trust as a platform quality combines three notions: security (or self-defense), trust, and fundamental host context. The ability for platforms to be on the high ground in comparison to the possible level of attacks that assault them goes without saying; likewise, when we hold the high ground, we do not want to yield this ground to the adversary or open up separate attack vectors that put this privilege in a position of compromise. A self-defense guarantee centers on the ability to verify and validate that some hierarchy of platforms can keep and hold the *cyber high ground*, even if one (or a number) of the platforms is in physical or operational control of an adversary. This defense guarantee logically includes a wide range of mechanisms from hardware-based physical protection schemes to protocol-level proofs of security where distributed cryptographic voting schemes may be employed.

Trust is an elusive concept because its definition is rooted in social concepts as opposed to technical. Despite the overloading of the term itself, we can use trust to express a quality that military commanders make quite frequently: an objective dependability (whether by mathematical proof or demonstrated testing) that a system will perform according to its specifications, even though negative consequences can occur. For our look into the future, we also use trust to describe high confidence that an adversary (whether inside or outside) cannot subvert the operation of a fleet of cyber defensive platforms. Depending on the description and expression of our security parameters, we may have some varying degree of trust expressed in terms of achieved security levels. These two views of trust (a system will perform as expected and confidence in an adversary's cost of compromise is extremely high) provide some context to consider design tradeoffs for future defensive architectures in the cyber realm. We may also consider other agent-oriented aspects of trust more common to information quality and collaborative agent societies, but we believe the more fundamental concepts have greater dominance for long-term system design.

In another workshop paper, we provide a closer look at how we may overlap system requirements analysis, attack modeling, and trust model specification to concretize a trust analysis space for Cybercraft. [6] To achieve the cyber high ground in the future, we must marry trust and security at some fundamental host context level. In other words, we need to consider the highest level of trust and security relative to the degree of independence from the host in which a cyber defensive platform operates. We can visualize an application-level platform that relies completely on the integrity of an underlying OS versus a possibly virtualized-level platform that sits possibly at the same level as an OS in terms of privilege. The virtualized approach affords the possibility for greater independence, but it still does not offer the highest level of independence because it may be open to (undetected) subversion. To get below the level of the OS or below the level of any possible hypervisor/virtual OS that may execute on a host, we must position the cyber defense platform at some fundamentally lower level where physical access to the hardware remains unhindered or unobscured. We are investigating the tradeoff spaces and design possibilities for such a hardware-based root of trust that would support the addition of synergistic physical protection mechanisms while giving a generic payload execution environment for defensive C3 packages.

We note that a fixed, hardware-based root of trust is not a new concept—the Trusted Computing Group (TCG) has sought such expression for quite some time. [7] TCG specifications give an initial set of security-related building blocks to link trust with various computational components, such as storage, networking, software, and devices. In considering future defensive cyber platforms, the military environment provides the business case and operational bounds for feasibly acquiring and implementing hardware-based manifestations of Cybercraft. The movement toward implementable and procurable secure hardware solutions in the commercial market at least demonstrates the overlap with USAF and DoD goals to integrate such technology. A root of trust established in hardware for future defensive platforms will give us the basis for analyzing other trust-related concepts, such as collaborative and adaptive decisionmaking problems where agents must consider varying levels of trust over time with the information they gain from other agents.

Highly Scalable C3 Architecture

If defensive platforms are to be truly useful, they must integrate seamlessly into networks to share information and increase their level of autonomy. We see this relationship expressed in the domain model of Figure 2, where Cybercraft platforms are related to other platforms (for C3 purposes) with no explicit realization given. As Figure 3 depicts, a conceivable (real world) USAF platform deployment hierarchy may be focused on traditional organizational units located at bases and managed by higher level network operations security centers (Integrated Network Operations Security [INOSC]/ Air Force Network Operations Center [AFNOC]). To operate with DoD and USAF relevance, platforms must communicate and coordinate functionally in networks of extremely large size. With a goal of one million or more such platforms residing on the same network, issues of scale become a dominating factor.

Suffice to say, there are very few networks in existence today that accommodate large-scale *and* complex C3. Three examples of large-scale networks are the Internet, GNUTella, and KaZaA, and each has a different topology and performance. The Internet follows a topology governed by several power-law relationships, [8] GNUTella employs a Peer-to-Peer (P2P) architecture, [9] and KaZaA uses a Hierarchical Peer-to-Peer (HP2P) architecture [10]. Many existing multi-agent architectures in fact fall into one of five categories: power-law, P2P, hybrid (HP2P), multi-layer, and hub-based. We may see glimpses of the future Cybercastle by looking at multi-agent communication topologies that currently scale to hundreds of thousands of clients—and we briefly describe each one along with positive attributes for consideration.

Power-Law Functions—During 1997–1998, researchers performed experiments to observe the traffic patterns at various points of the Internet. [8] As the Internet grew by 45% during this period, the observations remained consistent through that growth. Scientists discovered that the structure of the Internet closely followed a power-law relationship among several graph topology metrics: the diameter of the graph, the out-degree of any node, and the average out-degree of the nodes of the graph. When displayed together on a log-log plot, these attributes formed linear relationships. This display yielded the notion of network topologies in large systems, in particular the Internet, as following a *power-law* relationship.

Because such power-laws have been shown to support large-scale networks, it makes sense to instantiate a network topology for defensive cyber platforms that follow these laws. However, building a network topology generator requires constructing a single node at a time, with the impact of each node on the overall structure remaining hidden until much later in the algorithm. Only once a sufficiently large number of nodes exists can the topology's macroscopic properties be measured—thus limiting the efficacy of such organization for future platform aggregations.

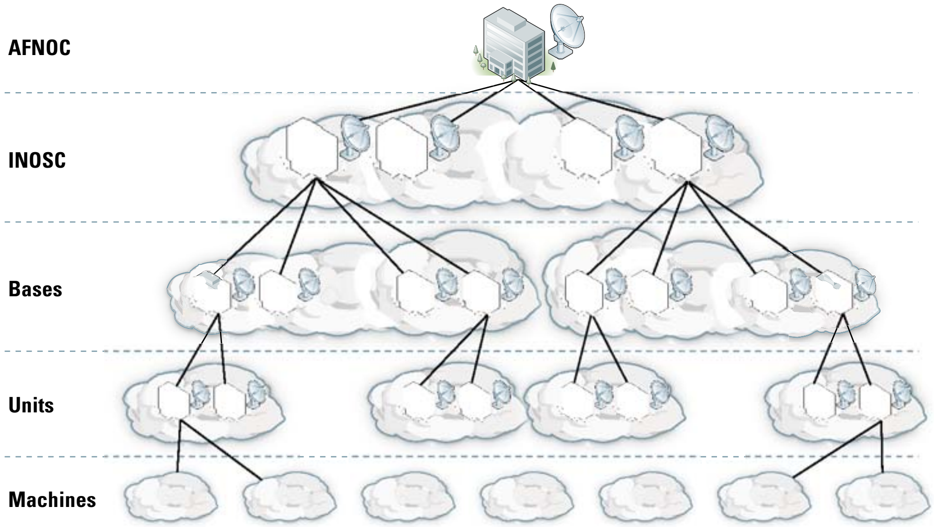


Figure 2 Conceptual Hierarchical Relationships Among Defensive Cyber Platforms

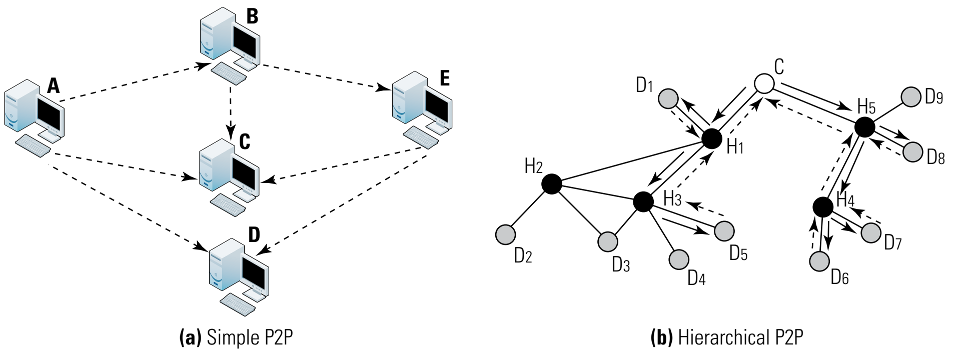
P2P Architecture—A P2P [9] network is one in which the nodes may establish multiple connections to other nodes. That is, the nodes are both client and server (or neither) and are free of the usual distinctions between the two. Rather, they communicate in a manner that best benefits the system objectives, without regard for the communication flow semantics of the client/server paradigm. A small P2P network is shown in Figure 3-a, illustrating that each node connects to as many other nodes in the network as deemed necessary. As we increase the number of connections per node, we reduce latency between source and destination nodes, but we also increase processing and communication burdens on all nodes along the source to the destination path.

The spanning form of a P2P network also nicely facilitates fault tolerance, where nodes may part and join the network dynamically and without warning. However, suboptimal network growth may adversely affect this fault tolerance. As a P2P network grows, it remains difficult to maintain a given set of performance metrics—and easily results in increased processing or bandwidth burdens on each node. Distinguishing between different types of nodes—*i.e., super* peer nodes—may offer a better hybrid approach.

Hierarchical P2P (HP2P) Architecture—An extension to the P2P structure includes super peers or super nodes. [10] These super peers act as regional hubs, absorbing additional burdens of the network traffic and processing load for distributed search and communications. These hubs may be interspersed across the network, as in the case of hubs controlling local clusters of regular nodes, or they may represent the bridges between layers of distinct P2P networks. The structure of the HP2P architecture improves on the P2P structure by incorporating clusters connected through super peers. These super peers provide additional bandwidth and processing capability similar to hubs, but because they are still multi-connected peers, they help retain the overall network structure. Such networks, as shown in Figure 3-b, are referred to as HP2P networks. P2P organizations scale to roughly tens of thousands of nodes, whereas HP2P has been shown to scale to approximately 50,000 nodes. [11] The benefit is that HP2P networks improve scalability by providing designated routes to other parts of the network. The clusters themselves are conveniently distinguished, allowing more intuitive segmenting of mission and information hiding from the rest of the network.

Botnet/Internet Relay Chat (IRC) Architectures—Often referred to as *botnets*, a *bot* (short for robot) *network* is a multi-agent distributed system that may be networked to other bots that possibly reside on a larger network (*e.g.,* the Internet) and is capable of being controlled by one or more users. One of the earliest uses of the term "bot" originates from IRC robots that were initially developed to run autonomously on IRC, allowing users to play games and performing simple authentication and chat channel protection functions. Botnets give us a small look at the power of organized agent societies that scale to large numbers of clients, and we can consider adaptations for cyber platform C3 topologies.

Though botnets were originally accessible only from IRC itself, they eventually offered the ability for users to log in and operate them with separate connections outside of IRC using proprietary protocols designed and tuned for C3. Thus, botnets were autonomous, operated in closed networks, and offered multiple interfaces for C3. They could also grow and shrink as bots became available or signed off. These features provide close corollaries to the desired features we wish to see in our future C3 defensive platform frameworks.



(a) Simple P2P

(b) Hierarchical P2P

Figure 3 Example P2P Network Configurations

Hub-Based Botnet Architectures—Hub-based architectures focus on a central point of communication, called a hub, to which one or more leaf nodes connect. The hub is responsible for all of the routing and usually much of the processing in the network. This design is still very popular for network hardware because it is simple and efficient for small- to medium-sized networks. It suffers from scaling problems, complexity in dealing with interconnected hubs, and networks in which graph cycles exist.

Botnets operating with a hub-based C3 structure have been known to connect 7,000 or more infected machines to a single IRC network at once. The ability to command an entire botnet at once is a significant capability to the botmaster. IRC networks as a means of botnet C3 are useful because of their simplicity, availability, and cost (free to botnet authors). They have since faded in use for malicious botnets because all communications and IP addresses can be logged, leading to discovery of how the botnets work and what purpose they serve. In addition, the authors and users of these botnets become vulnerable because they too must connect to IRC to interact with their bots.

Fast-Flux Botnet Architectures—Fast-flux is a relatively new DMAS architecture, leveraged extensively by cybercriminals to support identity theft, spam email, and perform other types of computer-based crime. [12] It exploits the deliberate configurations of some networks to allow rapid changing of dynamic IP addresses, such as those that support cable and dial-up users. The goal is for a fully qualified domain name to have hundreds or even thousands of IP addresses assigned to it. The IP address to which the hostname resolves is then changed between the IP addresses frequently, with a very short time-to-live parameter. This prevents caching of the IP addresses by Domain Name Service (DNS) servers and forces DNS clients to continually recheck for the most recent IP address of the target hostname. Users attempting to connect to the destination host will connect to a different IP often—sometimes on a minute-by-minute basis. The fast flux domain name can then be used to maliciously build a reliable network of hosts that serve Web pages that may or may not be infected with viruses, Trojans, or other malware.

Fast-flux networks can be further extended to multiple layers, where infected hosts serve as redirectors to backend content servers, called *motherships*, which serve both Hyper-Text Transfer Protocol (HTTP) and DNS, providing virtual hosting for up to thousands of different Top-Level Domains (TLD). Fast-flux networks with more than 400,000 nodes are believed to exist, [13] presenting a possible real-world example of functioning large-scale systems and a possible glimpse of what C3 may look like for cyber defense platforms in the next decade.

Extensible Agent Architecture

Secure root of trust and C3 requirements create a large separation between normal business class networks on which a typical DMAS might operate and the military context in which cyber platforms of the future will operate. As we discussed in our workshop paper, the uniqueness of the agent architecture for the future Cybercastle may also create a rich area of research and associated challenges. [14] We consider the requirements for the Cybercraft *platform* (essentially a lightweight agent with a possible realized manifestation in hardware), which receives and executes generic *payloads* based on a common interface. We envision these payloads to be modules that execute persistently in agent process space, such as system and network sensors or communications modules.

There are countless possibilities for the further decomposition of the domain concepts seen in Figure 1 for cyber platform/payload interaction. We may in fact consider a broad range of possibilities for how a cyber defensive platform may be decomposed to achieve the goals of secure root of trust, scalable C3, and generic execution of payloads to support network defense goals. In our current research, we investigate the use of a classic design pattern from robotic control theory model known as Three-Layer Architecture. [15] This paradigm is designed to support multi-staged information flow for core decisionmaking activities and is built on a planning approach, where each of the three layers of the agent's planning process attempts to break a complex plan into one or more simpler plans.

We illustrate a possible component-based Three-Layer Architecture that meets the high-level goals for a defensive platform collective in Figure 4. The *coordinator*, *sequencer*, and *controller* structures provide the necessary interfaces to allow payloads to produce, share, and respond to state changes in the environment. The *coordinator* (often called the deliberator) deals with high-level goals, the *sequencer* splits a goal into actions, and the *controller* framework carries out the actions using a perceptual state and a primitive feedback loop. This process supports the implementation of more sophisticated and longer term goals, as well as machine learning, on which future defensive cyber collectives will likely rely.

This architecture illustrates a layered approach to payload integration and command functions. The first stage of information flow involves sensor modules that collect data about the agent's local or global environment. Other modules for the first stage include modules that provide secure and encrypted channels of communication. The second stage manages local perceptual state modules. Because the application demands a small agent, the state tracking is minimal, based on current mission and policy. Learning and decisionmaking occur in the third stage. For this application, modules in the third stage implement the Unified Behavior Framework (UBF). [16] This behavior framework supports simple and aggregate behaviors and is designed to be modified at runtime—illustrating one possibility for introducing flexibility and extensibility into the platform design.

In this design, the behavior (or controller) carries out sets of actions designated by the sequencer and provides quick response to unexpected states (much like a human's automated responses to tripping over a stone). The UBF maps behaviors together to form aggregate behaviors, and the mapping can be changed at runtime. Architectural design such as this may help better express a commander's intent or an operator's policy expression, which may change frequently and unexpectedly based on the needs of the mission and the agent's autonomy level.

The final stage in this model is an actuator stage. This stage usually consists of communicating alerts and status information back to human operators. However, if the system is under attack or detects threats to mission or resources,

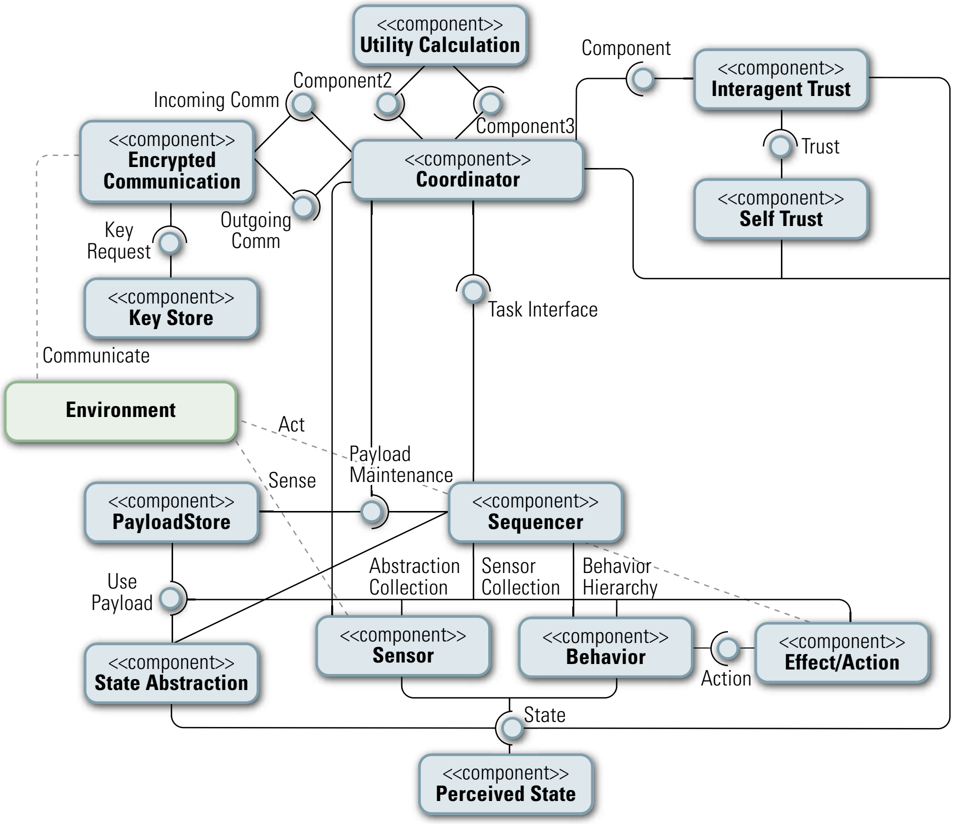


Figure 4 Conceptual Component Design for Defensive Cyber Architecture

Level	Synapsis
1	The computer offers no assistance; human must make all decisions and take actions
2	The computer offers a complete set of decision/action alternatives
3	The computer offers a selection of decision/action alternatives
4	The computer suggests one alternative and executes that suggestion if the human approves (management by consent)
5	The computer suggests one alternative and allows the human a restricted time to veto before automatic execution (management by exception)
6	The human is not involved in the decision making process; the computer decides and executes autonomously

Table 1 Levels of Computer System Automation

such as distributed denial of service, modules in this stage may restructure the network or enable additional security constraints. Secure communications is built into the core agent design, with a key store that will most likely be distributed. Models such as this express intent for agent architecture with flexible payload support and execution of defensive missions that may or may not exist when the fleet is deployed. The modules at each stage need only support the interface and communication requirements of the agent design. This provides a framework that may grow in capability as the system evolves and may be reconfigured at runtime.

We believe the strength of such robotic-based control design helps focus delineation of tasks in the platform and helps identify the possible interfaces between discrete components. This design also reflects the concept that our defensive platforms essentially function in the role of distributed and coordinated cyber sensor networks, with the added advantages of learning and large-scale communications. This particular design consideration offers us visibility into what the next generation of defensive agent collections will need to look like and helps us explore current technologies and design prototypes that may be integrated into a cohesive operational framework. Regardless of the particular agent design chosen, they will all need a high level of extensibility and flexibility to avoid monolithic platform/ payload realizations.

Autonomous Operations

Given flexibility in the agent architecture itself, questions remain about how, when, and where to permit human operators to observe and control the keys to the future Cybercastle defensive infrastructure. After all, attacks occur at the speed of electronic propagation, and detection/ response may need to execute at the same speed. Future systems will need some level of autonomy that our defensive cyber systems provide only in limited operational situations currently (*i.e.,* quarantining a known detected virus). Future defensive platforms must provide visibility and fusion of data *via* payloads so that the cognitive bandwidth of appropriate operators, administrators, and commanders remains low in the face of complex and coordinated network attacks. The effectiveness of the operator and the cyber platform network under consideration depends heavily on many factors, including the heterogeneity of the mission, the complexity of the interface to the cyber platforms, specific policies, the complexity of the payloads themselves, and the level of autonomy given to a cyber platform.

One common model for an operator control loop involves six levels of automation, as shown in Table 1. [17] Given a large network, a small number of centralized operators, the complexity of the USAF network defense mission, the number of varied activities in the future defensive landscape, and the speed of threats against this future integrated platform environment, it is unlikely that operators will be able to actively choose a course of action for each decision point (Level 1). Likewise, full software autonomy (Level 6) is unlikely due to the nature of the missions involved and trust evaluation of commanders at various levels. Research will continue to refine how we may effectively and efficiently inject operator monitoring and control into the fabric of the Cybercastle walls.

Redundancy/Fault Tolerance

Through normal incidents that create network outages in connectivity providers and lower reliability of some military systems (wireless, satellite), networks today and in the future will undoubtedly experience periodic connection problems. Whether our future defensive cyber platform hierarchies remain connected and operational in such environments is a question of great importance. Cyber defensive platforms in such network conditions must determine which missions are viable and how (if at all) the network must be reorganized. If a given set of missions cannot be completed, agent platforms must provide appropriate operator feedback or be programmed to execute autonomous decisionmaking evaluations. An operator may want to cease processing specific missions or provide for an autonomous halt so other missions remain unaffected. Cyber defensive platforms will be the workhorse to handle a wide variety of such network-related problems and will most likely act to provide correction, allow disconnected networks to rejoin, reevaluate traffic flows and patterns, and reorganize network configurations so missions can continue.

A plethora of research into distributed systems exists for determining when a network becomes disconnected and how to establish new leadership. The challenge for the Cybercastle of the future is determining if missions may continue based on more restricted resources. When loss of communication removes processing power, information, and assets that may be essential to completing the mission, we may allow our fleet of Cybercraft to know which resources are necessary to continue processing. How can we best represent these requirements? If the network is split evenly in two, each with the capability to continue the mission, should they both continue, should only one continue, or should both abandon processing? This provides yet another fertile ground of research, and the results will shape more precisely how defensive network suites function.

Looking Ahead

In the near term, there are several areas of achievable goals that we want to consider to develop and design the blueprints of the Cybercastle to meet the demands of the next few decades. Of interest will be the applicability of the HP2P design to military networks and our ability to formulate feasible options for hardware-based levels of trust in a host/system design context. Cyber platforms will need to be overlaid onto networks with varying underlying physical hierarchical topologies and possibly some independent communication networks for key super peer platforms of importance.

To integrate revolutionary concepts into the mainstream operational networks of interest (which our future C3 defensive systems will require to stay ahead of our adversaries), we must consider at some point how the transition from our current modes of operation might merge with newer technologies. We can start to gauge the design tradeoff space for the Cybercastle of the future by considering examples of current mission-critical systems, such as the Common Operational Picture (COP) and Air Operations Center (AOC). COP is a military system that distributes real-time information about a mission area (typically geography-centric) to personnel who use the information for mission planning. In a simplistic view, imagine a terrain map viewed on a desktop computer. The COP then feeds information about mission targets, friendly force locations (ground, air, and sea), points of interest, and other useful data overlaid onto the map. The information sent through the COP network typically consists of more than object position, and it allows operators to tie assets back to missions and vice versa. Such an integrated collection of missions may provide the perfect context for considering how revolutionary defensive changes may be integrated.

Regardless of what the Cybercastle physically looks like in 2020, we believe it must embody several of the principles we have discussed here: a secure root of trust that gives us the cyber high ground, a flexible C3 architecture that allows hierarchical and complex relationships among defensive nodes, and an extensible agent architectural design that supports tailored payload development and implementation with minimal changes to established platform interfaces. Of course, this collective must also provide some ease of use, support for autonomy, and resilience against network failure/attack. We believe some of the building blocks exist for this Cybercastle already: namely, our earnest expectation as researchers and cyber warriors to see them realized so the USAF may indeed fly, fight, and win in Cyberspace. ■

References

1. Gettle, M. "Air Force releases new mission statement." December 2005. *http://www.af.mil/news/story.asp?id=123013440.*
2. Lopez, C. T. "8th Air Force to become new cyber command." November 2006. *http://www.af.mil/news/story.asp?storyID=123030505.*
3. National Security Presidential Directive-54 / Homeland Security Presidential Directive-23 (Cybersecurity Policy).
4. Phister, D. P., Fayette, D., and Krzysiak, E. "Cybercraft: Concept linking NCW Principles with the Cyber Domain in an Urban Operational Environment." Technical Paper, Air Force Research Laboratory, 2006.
5. Kowalski, E. et al. "Insider Threat Study: Illicit Cyber Activity in the Government Sector." Technical Report, U.S. Secret Service and Software Engineering Institute, Carnegie Mellon University, January 2008. February 11, 2008. *http://secretservice.tpaq.treasury.gov/ntac/ final_government_sector2008_0109.pdf.*
6. McDonald, J. T., and Hunt, S. "Developing a Requirements Framework for Cybercraft Trust Evaluation." Proceedings of the 3rd International Conference on Information Warfare and Security, April 2008.
7. Trusted Computing Group, TCG Specification Architecture Overview. Revision 1.4 2 April 2007. *https://www.trustedcomputinggroup.org/groups/TCG_1_4_Architecture_Overview.pdf.*
8. Faloutsos, M., Faloutsos, P., and Faloutsos, C. "On power-law relationships of the internet topology." SIGCOMM, 1999, pp. 251–262.
9. Foster, I. T. and Iamnitchi, A. "On death, taxes, and the convergence of peer-to-peer and grid computing." IPTPS, 2003, pp. 118–128.
10. Yang, B. and Garcia-Molina, H. "Designing a super-peer network." ICDE, vol. 00, p. 49, 2003.
11. Ripeanu M., Iamnitchi, A., and Foster, I. "Mapping the gnutella network." IEEE Internet Computing, vol. 6, no. 1, 2002, pp. 50–57.
12. KYE, "Know your enemy: Fast-flux service networks." The Honeynet Project & Research Alliance, White Paper, July 2007.
13. "Kraken botarmy." [Online]. *http://www.damballa.com/research.*
14. Karrels, D. R. and Peterson, G. L. "CyberCraft: Protecting Air Force Electronic Systems with Lightweight Agents." Vir V. Phoha and S.S. Iyengar (editors), Proceedings of the Cyberspace Research Workshop, 58-62. United States Air Force, Shreveport, LA, November 2007.
15. Gat, E. Artificial Intelligence and Mobile Robots. Cambridge, MA, USA: MIT Press, 1998, ch. On Three Layer Architectures, pp. 195– 210.
16. Woolley, B. G. and Peterson, G. L. "Genetic evolution of hierarchical behavior structures." GECCO '07: Proceedings of the 9th Annual Conference on Genetic and Evolutionary Computation. New York, NY, USA: ACM, 2007, pp. 1731–1738.

▷▷ *continued on page 19*

IATAC SPOTLIGHT ON FACULTY

Capitol College 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. The SMEs profiled in this article are Dr. Vic Maconachy and Mr. Allan Berg of Capitol College.

In October 2007 Dr. Maconachy assumed the position of Vice President for Academic Affairs and Chief Academic Officer, where he is charged with sustaining and enhancing the academic quality of programs of study ranging from business administration to engineering, computer science, and information assurance. He also oversees the operations of the Innovation and Leadership Institute, Office of Academic Research, Library, and Space Operations Institute.

Before joining Capitol College, Dr. Maconachy held several leadership positions at the National Security Agency (NSA). He was appointed by the Director of the NSA as the Deputy Senior Computer Science Authority, where he built a development program for a new generation of Cryptologic Computer Scientists. Before this position, Dr. Maconachy served as the Director of the National Information Assurance Education and Training Program (NIETP). He was responsible for implementing a multidimensional interagency program, providing direct support and guidance to the services, major Department of Defense (DoD) components, federal agencies, and the greater national information infrastructure community. This program fosters the development and implementation of information assurance training programs as well as graduate and undergraduate education curricula. In this capacity, he served on several national-level government working groups and in an advisory capacity to several universities. Dr. Maconachy was the principal architect for several national Information Security (INFOSEC) training standards in the national security systems community. During Dr. Maconachy's time at the NSA, he held many different positions, including INFOSEC Operations Officer, INFOSEC Analyst, and Senior INFOSEC Education and Training Officer.

Before joining the NSA, Dr. Maconachy worked for the Department of Navy. He developed and implemented INFOSEC training programs for users and system maintainers of sophisticated cryptographic equipment. He also served as the Officer in Charge of several INFOSEC-related operations, earning him the Department of the Navy Distinguished Civilian Service Medal. Dr. Maconachy is also a founder, past chair, and member of the National Colloquium for Information Systems Security Education. Dr. Maconachy holds a PhD from the University of Maryland, has written numerous publications and earned awards related to information assurance, and has received the prestigious National Cryptologic Meritorious Service Medal. [1]

Mr. Allen Berg is the Assistant Dean for Graduate Studies and Director of the Critical Infrastructures and Cyber Protection Center. Before joining Capitol College, Mr. Berg was the Director of Information Assurance and Infrastructure Protection Programs at Towson University, and he was an assistant professor and Deputy Director of the Center for Information Assurance at the University of Dallas Graduate School of Management. Before joining the University of Dallas, Mr. Berg served as an Associate Director of the Institute for Infrastructure and Information Assurance and the Deputy Director of the Commonwealth Information Security Center in the College of Integrated Science and Technology at James Madison University (JMU). During his tenure at JMU, he was instrumental in developing the remote-learning MS in computer science concentrating in information security and the remote-learning MBA concentrating in information assurance. In addition, he developed and implemented marketing strategies that forged educational relationships between the university, corporations across the country, DoD, federal and state government agencies, and other educational institutions. Mr. Berg served as a member

▷▷ *continued on page 19*

Securing the Converged Enterprise, Part 2

Network Defense-in-Depth Architectural Considerations

by AT&T

The Vanishing Network Perimeter

Converged enterprise networks bring together a wide variety of applications, protocols, devices, and underlying network types. The result is a communications environment in which employees are no longer restricted to using network services from traditional office workstations. Instead, they now frequently access voice and data network application services while traveling and at home. The traditional enterprise network "perimeter" is disappearing, and network access now extends to just about everywhere. Separate networks are joining together to provide a seamless experience that does not require users to stop and restart a data or voice session when they change locations. Corporate network security must adapt to support this transition.

Historically, the intersection of the public Internet and the private corporate campus local area network (LAN) has been considered the one and only network perimeter and the most vulnerable spot in the network because the Internet is a publicly accessible network. The Internet also falls under the management purview of multiple network operators, rather than individual enterprise network managers. Therefore, it is considered an "untrusted" network.

This network junction should continue to receive access control, firewall, and intrusion detection and prevention filtering protection. Today, a full defense-in-depth approach to security has become an industry best practice. With a defense-in-depth approach to security, multiple security points are placed between the user of the data and where the data is processed and stored, helping enterprises better deter both internal and external attacks against their network or data. Attacks may vary in nature, with each requiring a different technological solution. The defense-in-depth security model helps protect against several different types of risks and reaches beyond the traditional network perimeter to permeate the wide area network (WAN), internal wired and wireless LANs, corporate servers, end-user computing devices, and enterprise data.

One recommended best practice for implementing defense in depth is to use a centralized management model, which involves automatically deploying software updates network-wide, in line with corporate policy, from a network operations center (NOC) or security operations center (SOC). This approach provides a substantial degree of automation that helps keep security, application, and operating system software updates synchronized. Keeping updates current becomes increasingly important as networks scale larger. A missed update could leave a chink in network armor, making centralized and automated update processes far more reliable and safe than a manual or ad-hoc process.

Identifying and Helping to Protect Network Trust Boundaries

If a concrete network perimeter no longer exists, how do you identify and strive to protect multiple network perimeters, or trust boundaries, that may be invisible? The answer lies with first identifying the various places where data is stored and used, such as in servers and client computing devices, and then considering the various ways potential internal or external attackers might cause harm, such as by—

- Attempting to gain unauthorized access to resources
- Listening to or capturing packets in transit
- Flooding network servers or devices with corrupt packets to create a denial-of-service (DoS) or distributed DoS (DDoS) attack that could overwhelm the devices and render them inoperable.

Externally, firewalls and intrusion prevention systems (IPS) join with encryption and endpoint security capabilities to help protect against data theft, unauthorized access, and the release of infected code (malware, such as worms) that remote and mobile devices might pick up from the public Internet. Internally, virtual LANs (VLAN), firewalls, and IPSs help thwart breaches between departments, between LANs, and between LANs and servers.

Let's take a closer look at these various solutions, how they function at each network segment, and some deployment options and considerations.

External Defenses

External defenses are designed to help protect data and voice traffic in transit over the WAN, thwart unauthorized external access to internal resources, and keep private sensitive data stored in mobile computing devices confidential. Protecting the traditional network perimeter at WAN access points in the data center and at branch and remote offices falls in the "external defense" category. External defense also includes measures taken to protect data in transit and endpoint or client device security.

Break-Ins and Malware

To protect physical LAN-WAN intersections such as at data centers, branch locations, and home-office locations, installing a series of gateways between users and data resources is recommended. In many cases, virtual private network (VPN) providers offer this service to help ensure a private device never directly exposes its own IP address to the public Internet, public switched telephone network (PSTN), or other shared network. The idea is to install layers of security between the user and resource, making it more difficult for potential malicious hackers to discover the IP addresses of an enterprise's servers and routers and break into them to cause mischief. If considering a gateway service, businesses should discuss with their service provider the appropriate number of gateways needed to achieve the desired level of security. Businesses should also address fees associated with the creation of multiple security layers.

Similarly, firewalls and IPSs are designed to protect connections at specified enterprise locations. Businesses can install and manage these devices at every site or purchase a managed service from a carrier. Alternatively, a network-based service (which does not require a CPE purchase) can be used to filter traffic against user access control lists (ACL) and other enterprise criteria at the service provider point of presence. The point of presence is where the enterprise access connection either meets a Multi-Protocol Label Switching (MPLS) backbone used for VPN services or meets the edge of an Internet service provider's network where encryption is applied to create an Internet VPN.

As noted, firewall and IPS filtering can be conducted at each enterprise WAN access point. However, this solution is less scalable. Having the service directly in a provider's backbone network allows businesses to scale these security capabilities as users and sites are added to the network. By filtering "bad" traffic from the network before it traverses the last-mile access link, identified unauthorized access attempts and malware are segregated from the network and its internal IP addresses. Keeping the malicious traffic at a distance helps reduce the likelihood of it harming the network.

Monitoring for Internet Threats

To further defend the WAN, emerging public Internet scanning services that help detect precursors to worms and other malicious events are available. The service is designed to then notify users of the pending vulnerabilities. Other services can specifically examine individual Internet or VPN traffic and potentially detect a DDoS attack aimed at an individual network. Some managed services will automatically deploy policies and take action to mitigate risks when certain events are detected on an individual VPN.

Encryption of Data in Transit

For added privacy protection of the data in transit, encrypted VPNs should be used in cases where traffic traverses the public Internet infrastructure. Encryption scrambles data and authentication information to create a private "tunnel" for each customer through the publicly shared Internet to protect the privacy of data in transit.

The VPN can be in the form of an IPSec VPN service between fixed corporate sites or a Secure Sockets Layer (SSL) VPN service for remote and mobile users.

Both SSL VPN and IPSec VPN support encryption, data integrity, and authentication technologies, such as Triple-DES, 128-bit RC4, Advanced Encryption Standard (AES), MD5, and SHA-1.

IPSec VPNs operate at Layer 3 and are recommended for static, "trusted" private enterprise sites that require LAN access on par with the primary site. IPSec encryption can be delivered in the form of a service that encrypts traffic across the service provider's backbone and utilizes a carrier's economies of scale as a business's number of sites and traffic volumes grow. Alternatively, VPN termination equipment can reside on the premises and can be installed and managed individually or by a carrier in the form of a managed network service. To help protect the network, security controls should be placed between the VPN egress point and the enterprise network.

For mobile workers requiring "on the fly" encryption, SSL VPNs may be a good choice. Because they are browser based, require no installation or maintenance of special client-side software, and offer application-layer access control, SSL VPNs can be quickly deployed. Unlike IPSec VPNs, SSL VPNs encrypt and decrypt at Layer 7 (see OSI model illustration).

Encryption and MPLS VPNs

MPLS technology creates virtual circuits that keep one customer's traffic from intermingling with another's. Encryption over these types of VPNs is not necessarily needed but is recommended for companies with the highest security requirements, such as those transmitting sensitive customer data. Services are available to encrypt traffic across the LAN or a shared MPLS backbone network segment.

Endpoint Security

Endpoint security involves creating policies for end-user computing devices, such as laptops, handhelds, and smartphones. The policies should cover—

- Update status of the device software programs
- Frequency of device scanning by central NOC or SOC to check for out-of-date software
- Protection against viruses and other malware
- Use of personal firewalls and host-based IPS software on the device
- Data protection through data rights management (DRM) solutions.

In the case of personal firewalls and host-based IPSs, consider the mobile device almost as a mini-network unto itself. It has an IP address for accessing the Internet. Without a personal firewall, the IP address is exposed directly to the Internet. Someone could find the IP address and compromise the system if the intruding system's own source address is not filtered off the network. The same holds true with host-based IPSs: someone could inject malicious code onto the computing device, either to cause harm to the device itself or to potentially infect the corporate network the next time the device connects to it.

Those policies can be enforced internally or through a carrier service that matches incoming service requests from mobile devices to a corporate policy. The policy resides in either an appliance or router in the data center and the scanning can take place there. Industry-wide, router and antivirus software makers have teamed together to build antivirus capabilities into common network equipment that scales to cover many devices as they attempt to access the network.

Policies can also be uploaded from the data center to a service provider's NOC or SOC, where incoming requests are scanned on behalf of the business to help keep "bad" traffic further from network components. The scans compare the software versions residing on the devices with the corporate mandate. If there is a match, the connection is allowed. If not, the IPS technology takes the action as dictated by policy to block the connection, update the software, or quarantine the connection for later remediation.

Other variables can be part of the policy as well, such as what type of connection the device is using to connect. Certain types of connections might be restricted from accessing certain resources. Similarly, there might be different policy requirements for guest access and for extranet users (business associates who you allow access to some of your network resources).

Internal Defenses

The primary goal of deploying internally focused security layers is to enforce enterprise policies regarding users' access rights. Layer 3 (see OSI model illustration) firewalls are used in a number of places to help verify that only authorized users gain access to the network by matching corporate policies of users' network access rights to the connection information surrounding each access attempt. If there is no match, the firewall blocks the connection.

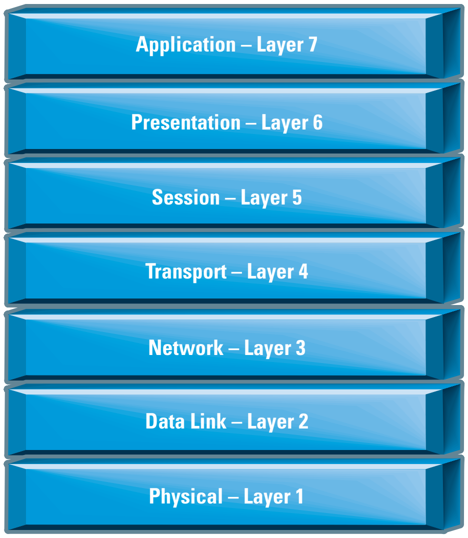
Segregating Departments

Many enterprises create VLANs to logically segregate user access to various corporate resources across their LAN. Enterprises often classify users and place them into segregated VLANs by department, but they can also create VLANs using another corporate criteria, such as a job title. In some cases, guests are placed into a "guest VLAN," and those users might not have access to anything but the public Internet.

Employees, guests, and extranet associates and vendors might represent a high-level classification of users, and employees may be further subdivided. Each classification is placed in its own VLAN, with access limited to resources specific to that user group. Similarly, Voice over IP (VoIP) traffic is usually placed in a separate voice VLAN with access limited to the corporate PBX (see "Securing the Converged Enterprise, Part I" for a discussion about securing voice traffic).

VLANs usually aggregate in Ethernet switches in the distribution layer of the corporate network. These switches reside

OSI Model



OSI is considered the primary architectural model for inter-computer communications. Layers 1–3 handle data transport issues. Layers 4–7 deal with applications. The layers are as follows—

- **Layer 1**—Physical Layer. Is the physical medium by which the customer information and packets are transported from origination to destination (OC3, cable, wireless, LAN, copper, SONET, private line)
- **Layer 2**—Data-Link Layer. Transports frames across the physical layer and provides transmission error notification (Frame Relay, ATM, Ethernet)
- **Layer 3**—Network Layer. Provides routing and related functions that enable multiple data links to be combined into an inter-network (routing protocols [BGP], IP, VPN, VPLS, MPLS)
- **Layer 4**—Transport Layer. Provides end-to-end transmission correctness, data recovery, and flow control using (Transmission Control Protocol [TCP] and User Datagram Protocol [UDP])
- **Layer 5**—Session Layer. Establishes a session (allows two networked resources to hold ongoing communications across a network) and security (SQL, Net BIOS)
- **Layer 6**—Presentation Layer. Determines how computers represent data; ensures information sent from the application layer of one system will be readable by the application layer of another system (data compression, data encryption, format conversion, use of image, ASCII, MPEG)
- **Layer 7**—Application Layer. Generates or interprets data (File Transfer Protocol, Simple Mail Transfer Protocol, electronic mail, Web browser).

between wiring closet switches and core data center switches. In this location, businesses should deploy protection against members of a VLAN gaining access to another VLAN's off-limits resources. These areas are locations where firewall filtering plays a role.

Firewalls represent the first level of access checking. They will either grant or deny a given IP address access to a resource. Deploying them at key "entry" points, such as where VLANs come together, where public and private networks meet, and where wireless and wired networks meet, reinforces corporate access policies to help ensure individuals see only the data they are supposed to see.

Many firewalls now also support application-layer inspection at Layer 7 (see OSI model illustration) for performing IPS capabilities, which check for anomalous protocol behavior. They also identify applications that attempt to "sneak" through the firewall at Layer 3 by hopping across TCP ports or by piggybacking onto the open TCP port 80 (defined to carry Web traffic).

Locations where a switch or router links one network or network segment to another form trust boundaries. A trust boundary is a vulnerable network border that provides an opportunity for a hacker or malicious code to enter the network. Each trust boundary represents a potential point of entry for a clever hacker. Firewalling and IPS capabilities, at a minimum, should be present at each of these boundaries.

Where Wired and Wireless LANs Meet

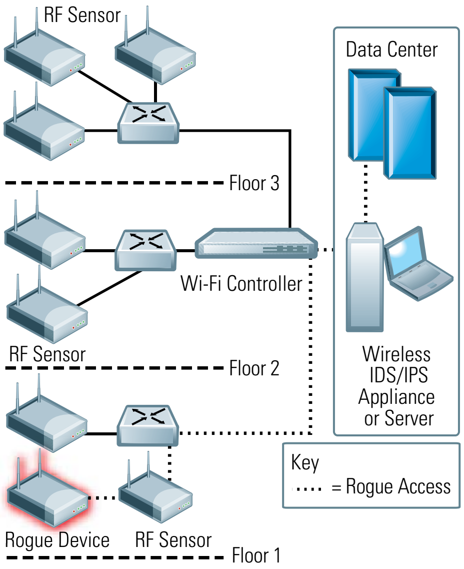
There is a juncture where 802.11-based wireless LANs (WLAN), also called "Wi-Fi" networks, meet the wired LAN. Security mechanisms built into Wi-Fi access points (AP), controllers, and client devices cover user authentication and encryption of passwords and authentication messages at the lower two OSI layers. However, as another trust boundary, this point in the network should also be checked to ensure wireless users match their wired access network rights and to prevent the malicious code from getting onto the network via the wireless network.

Some WLAN systems have per-user firewalls built directly into them. Others do not, requiring wireless users to pass through either the central NOC/SOC firewall or a firewall appliance that front-ends the WLAN controller. Some large networking vendors that participate in both wired and wireless markets have integrated the systems to a point where security devices on the wired LAN (whether managed internally or by a service provider) communicate with the WLAN controller, thereby applying both wireless and wired security protection capabilities to the radio frequency (RF) traffic.

Wi-Fi networks operate in unlicensed spectrum, which means anyone can use these frequencies as a network medium, even if they potentially interfere with another network. Wireless, which radiates in three dimensions, is less controllable and traceable than wires that plug directly from user computers into Ethernet switch ports. Radio waves can leak outside the building, making it possible for an attacker to piggyback on a user connection and gain access to the corporate network. Theoretically, if wired authorization, authentication, and accounting (AAA) measures are rock solid, they will help prevent attackers from coming in through the wireless back door. At this point in time, that is not a risk most enterprises are willing to take.

Wireless IPSs that operate at the RF level to detect unauthorized (rogue) devices can be deployed as an integrated part of a WLAN system, an overlay monitoring system operated in house, or a third-party service (see wireless IDS/IPS illustration). Many can detect whether the rogue device is actually connected to the corporate network. Rogue devices that are connected are more dangerous because such a connection means an unauthorized device has established a potential path to network resources. Unconnected rogues might simply belong to a nearby network operator.

Sample Configuration of Wireless IDS/IPS



Even if a rogue access point is not connected to the network, it is still a red flag. It might try to connect to the network or lure a client device to the network.

Wi-Fi clients are designed to associate to the wireless access point with the strongest signal. If the client associates to a malicious rogue, the rogue can flood the client (or the network to which the client connects) with messages to cause a DoS attack. In an effort to capture that user's credentials, the rogue access point may also lure the user to a phony Web site that appears to be the real thing. This is a breach called phishing.

Most wireless IPSs alert businesses to issues surrounding rogue activities and have the capabilities to automate the process of shutting down a rogue. Caution should be exercised with that option, particularly if the network is in a multi-tenant building or a fairly populated environment. The detected rogue might be a legitimate device in use by the business down the hall or the residence next door. Automatically shutting down these devices could create other issues.

When using wireless IPS systems, it is important to program them so they continually scan all worldwide channels—even those not sanctioned for use in the company's own particular country. Otherwise, the rouge access point might be overlooked.

Conclusion

Convergence is happening across devices, networks, protocols, and applications. This integration affords business users many productivity and time-saving benefits and entirely new communications capabilities not previously possible. However, because employees increasingly work in branch offices, in home offices, or in a mobile fashion from anywhere on the road, there is no longer a single network perimeter to protect. Instead, there are multiple, invisible network edges that need defending as users access the corporate network from many locations (both trusted and untrusted) and start to store sensitive data in their mobile computing devices.

Because of the distribution of users and computing devices, applying security measures to the converged enterprise has become a multi-dimensional discipline that requires a defense-in-depth approach to network security to help protect against various types of risks, such as—

- Unauthorized access to resources
- Theft of data packets in transit
- Break-ins to personal computing devices
- Introduction of viruses and other malware onto the corporate network that could render one or more systems inoperable
- Unauthorized use or alteration of enterprise data.

Centralizing the functions of pushing software updates and managing access control, firewalling, and intrusion protection helps ensure an enterprise consistently enforces a single corporate policy or set of policies network-wide. This centralization also allows security measures to scale as the network and number of users and devices grow. CPE can be installed and managed in house or through a service provider in the form of a managed service. Alternatively, a WAN service provider can deploy and manage a centralized, multi-layer defense from its own NOC or SOC in the form of a service. In this scenario, rules and policy engines in the corporate data center communicate with the provider's NOC or SOC, where they are enforced.

The traditional network perimeter has vanished and the convergence of different traffic and application types on a common network means putting many more "security-related eggs" into a single basket. A threat to the data network, for example, has suddenly become a threat to the voice network, too. These conditions are challenging enterprise IT departments to build a comprehensive, multi-dimensional foundation that uses a mix of services, products, policy, and network automation to cast a strong net of security measures across their organizations' dynamic and ever-evolving communications infrastructure.

Key Points to Securing a Converged Environment

- Utilize the network as a security device
- Deploy a centralized defense-in-depth architecture for consistent enforcement of policy and scalability
- Aim to detect and block malware on the endpoint and in the network
- Use strong authentication with users
- Help protect data using multiple solutions, including DRM, encryption, and access control
- Take both preventative and near real-time measures to help protect data. ■

References

1. Web: *http://en.wikipedia.org/wiki/Osi_model. For more information on this topic, visit http://www.att.com/networkingexchange.*

For additional information about this topic, visit *http://www.att.com/networkingexchange* or call Mary Forbes 443/896-5221 AB-1051-01

▷ continued from page 12

17. Sheridan, T. B. and Verplank, W. L. "Human and computer control of undersea teleoperators." MIT Man-Machine Systems Laboratory, Tech. Rep., 1978.

About the Authors

Lt Col J. Todd McDonald | is an Assistant Professor of Computer Science in the Department of Electrical and Computer Engineering at AFIT. Lt Col McDonald received a BS in computer science from the US Air Force Academy, an MS in computer engineering from AFIT, and a PhD in computer science from Florida State University. His research interests include software protection, obfuscation and anti-tamper applications, network and information security, and secure software engineering.

Dr. Gilbert "Bert" Peterson | is an Assistant Professor of Computer Engineering at the AFIT. Dr. Peterson holds a BS in architecture, an MS in computer science, and a PhD in computer science from the University of Texas at Arlington. He teaches and conducts research in digital forensics and artificial intelligence.

Capt Daniel R. Karrels | is a computer engineering PhD student at AFIT. Capt Karrels received his BS and MS in computer engineering from the University of Florida. His research interests include artificial intelligence, networking, large-scale systems, object-oriented design, and data structures.

Major Todd R. Andel | is an Assistant Professor of Computer Science in the Department of Electrical and Computer Engineering at AFIT. Major Andel received a BS in Computer Engineering from the University of Central Florida, an MS in Computer Engineering from AFIT, and a PhD in Computer Science from Florida State University. His research interests include formal methods, wireless routing, and network security protocols.

Dr. Richard "Rick" Raines | is the Director of the Center for Cyberspace Research (CCR) at AFIT. Dr. Raines received a BS in electrical engineering from Florida State University, an MS in computer engineering from AFIT, and a PhD in electrical engineering from Virginia Polytechnic Institute and State University. He teaches and conducts research in information security and global communications.

▷ continued from page 13

of the Virginia Alliance for Secure Computing and Networking Project (VASCAN), which was created to help secure Virginia universities and to work with the Virginia state government to aid in developing secure Virginia initiatives.

Mr. Berg has more than 35 years of experience in the intelligence community, private industry, and higher education. His experiences include developing security education programs for industry and the military on operations security and physical and personnel security. Mr. Berg has served as a consultant to universities and community colleges where he assisted in developing information security programs and federal grant proposals. His expertise includes distance education, security management and training, all-source intelligence collection and analysis, diplomatic activities, and special operations. Mr. Berg's work with universities and community colleges, the business community, researchers and faculty, and federal funding agencies has given him a deep appreciation of the importance of forging and supporting educational relationships between community colleges and universities and federal and state governments to meet the nation's commitment to securing our country and the protection, safety, and well-being of its citizens.

Mr. Berg is a member of the Government Security Conference (GOVSEC) board of advisors and served as the GOVSEC 2003 National Chairman. In addition, he is the Director of the Colloquium for Information Systems Security Education Secretariat, as well as the Treasurer and Conference Manager.

If you have technical questions for Dr. Maconachy, Mr. Berg, or another IATAC SME, please visit *http://iatac.dtic.mil/iatac*. The IATAC staff will assist you in reaching the SME best suited to helping you solve the challenge at hand. If you have any questions about the SME Program or are interested in joining the SME database and providing technical support to others in your domain of expertise, please email *iatac@dtic.mil* to have the URL for the SME application sent to you. ■

References

1. Web: *http://www.cisse.info/colloquia/cisse12/program/Vic%20Maconachy.htm.*

About the Author

Angela Orebaugh | supports a variety of security engagements with the National Institute of Standards and Technology (NIST). She has 15 years 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*

Common Criteria Testing Continues to Improve Security of IA Products

by Steve Rome

Public and private parties have been conducting product evaluations ever since products originated. The degree of trust in those evaluations is dependent on the evaluator's expertise and objectivity. Government laboratories generally have a high degree of public trust, but they may not operate at competitive rates. The US Government did not initiate testing of commercial information assurance (IA) products until the late 1970s, but their inability to test an exponential rise in security products gave rise to commercial laboratories. This article discusses how the International Common Criteria (CC) Standard meets that need.

Since 2000, Common Criteria Test Laboratories (CCTL) have been conducting evaluations of IA products under the National Information Assurance Partnership (NIAP); overwhelmingly, results have indicated that the security of these products has improved. The Common Criteria Evaluation and Validations Scheme (CCEVS), which is the US implementation of the International Common Criteria Standard (International Organization for Standardization [ISO] 15408), is flourishing with more than 100 ongoing evaluations and nearly 300 evaluations completed to date.

History of Evaluations

In the 1980s, the US Government evaluated products against security criteria under the Trusted Products Evaluation Program (TPEP). Later, the Trust Technology Assessment Program (TTAP) became a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to commercialize the evaluation of commercial off-the-shelf (COTS) products at the lower levels of trust. Under the auspice of the National Voluntary Laboratory Accreditation Program (NVLAP), TTAP accredited and provided oversight of commercial evaluation laboratories focusing initially on products with features and assurances characterized by the Trusted Computer System Evaluation Criteria (TCSEC) B1 and lower levels of trust. European Community evaluations were performed under the purview of national test standardization bodies associated with NVLAP. The TTAP was established to transition from TCSEC-based evaluations to CC-based evaluations under a common evaluation methodology.

In the 1990s, European-developed criteria were filling a role roughly equivalent to the TCSEC and Information Technology Security Evaluation Criteria (ITSEC). Canadian Trusted Computer Product Evaluation Criteria was the Canadian equivalent of the TCSEC. In January 1996, The CC, a multinational effort to write a successor to the TCSEC and ITSEC that combines the best aspects of both, was released. In the United States, 120 product evaluations were conducted under TPEP and TTAP during a 16-year period, with an average cost to the US Government exceeding $1 million per evaluation/validation. During that time, a typical C2 (roughly equivalent to today's Evaluated Assurance Level [EAL] 2 or 3) product evaluation required between 1.5 years and 3 years to complete.

EAL refers to the functional or assurance claims in predefined packages. For example, EAL 1 means that the product has been functionally tested using available off-the-shelf vendor documentation. EAL 4 means the product has been functionally tested with insight into the design and comprehensive test coverage. Testing was supported by an independent search for obvious vulnerabilities. An EAL 7 evaluation would mean more formal methods and systematic covert channel analysis was performed. These products must be modular and layered in design, and an independent search for vulnerabilities by an attacker with high-attack potential is accomplished by NSA.

History of the Common Criteria

In 1994, the United States joined the Europeans and Canadians to develop the first version of the international CC. In 1999, the ISO adopted the CC and became ISO 15408. Then in 1998, the Common Criteria Mutual Recognition Arrangement (MRA) was established with initial signatories: Canada, France, Germany, the United Kingdom, and the United States. Australia and New Zealand joined in

1999, followed by Finland, Greece, Israel, Italy, the Netherlands, Norway, and Spain in 2000. Under MRA, each member nation mutually recognizes and accepts evaluations against the Common Criteria standard accomplished at CC EALs 1–4. The original MRA was signed in 1998 by Canada, France, Germany, the United Kingdom, and the United States. Australia and New Zealand joined in 1999, followed by Finland, Greece, Israel, Italy, the Netherlands, Norway, and Spain in 2000. The arrangement has since been renamed Common Criteria Recognition Arrangement (CCRA), and membership continues to expand. The European Union countries within the former ITSEC agreement also typically recognize higher EALs. Evaluations at EAL5 and above often involve the security requirements of the host nation's government; in the United States, NSA conducts additional testing.

Nations can sign up to accept evaluations that member nations perform (certificate consuming), and they may become certified to conduct evaluations (certificate producing). Figure 1 illustrates the current 24 signatories. Italy is working to become a certificate-producing nation in 2008. Many other nations have inquired about joining the CCRA.

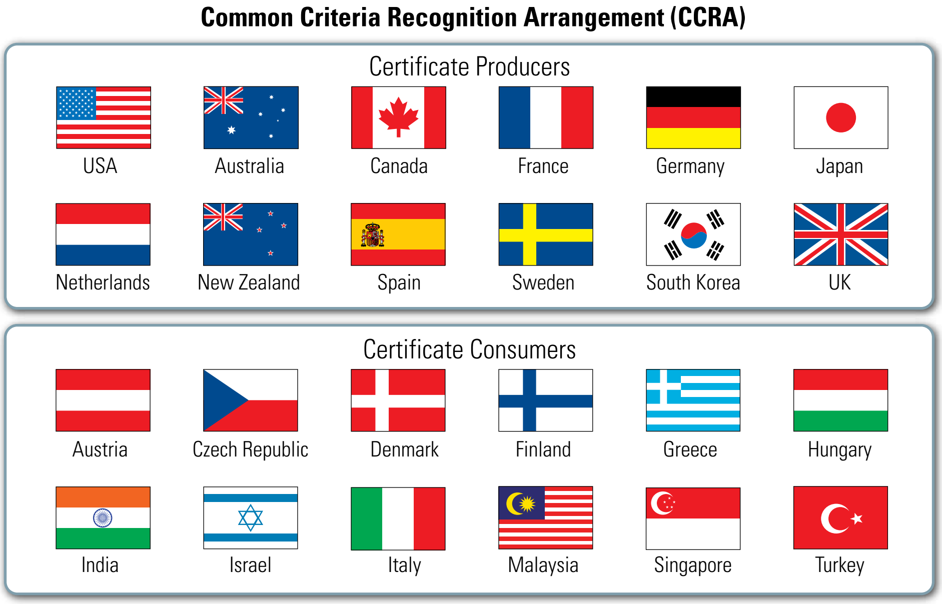


Figure 1 Signatories of CCRA (March 2008)

US Policy

The National Security Telecommunications and Information Systems Security Committee (NSTISSC), now known as the Committee on National Security Systems (CNSS), published the National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, Subject: *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products*, in January 2000 and revised it in June 2003. For the US national security community, it mandated that all COTS IA and IA-enabled products be evaluated by at least one of the following—

- International Common Criteria MRA
- NIAP Evaluation and Validation Program (CCEVS)
- NIST Federal Information Processing Standard (FIPS) validation program.

To learn more, readers may wish to read the fact sheet at the following website *http://www.cnss.gov/Assets/pdf/nstissp_11_fs.pdf.*

In October 2002, Department of Defense (DoD) Directive (DoDD) 8500.1 was issued mandating compliance with NSTISSP 11, which requires that products be evaluated or in evaluation (with successful evaluation a condition of the purchase). In February 2003, DoD Instruction 8500.2 mandated that products being evaluated also conform to a Government Protection Profiles (PP) (whenever one exits). Government PPs identify sets of security and assurance requirements for specific technology types. A PP is a combination of threats, security objectives, assumptions, security functional requirements (SFR), security assurance requirements (SAR), and rationales. For current validated US PPs, visit the US Scheme at the following website *http://www.niap-ccevs.org/ppl.*

For US Government entities not in the national security community, NIST published *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products* (Special Publication 800-23) in August 2000. These guidelines apply to all US Civil Government and recommend CC evaluations and validations. See *http://csrc.nist.gov/publications/PubsSPs.html.*

Common Criteria Today

In the United States, CCEVS oversees the nine accredited CCTLs that are currently conducting more than 120 product evaluations. Figure 2 illustrates the current NIAP laboratories. Information about each laboratory can be found at the following website: *http://www.niap-ccevs.org/cc-scheme/testing_labs.cfm.*

Of the roughly 300 products that have completed evaluations, the security posture of most has been improved. A typical evaluation not only improves the documentation but also usually finds areas that vendors correct in the product as a result of penetration and other testing. Laboratories work closely with clients to improve their products. Security improvements have greatly reduced vulnerabilities in products, and our clients believe that the CC experience provided value. Evaluation levels have been focused higher over the past year, but all US laboratories have experienced a steady flow of new and repeat clients as the US Government and private industry embrace NSTISSP 11.

For insight into evaluations that other CC member nations have conducted, visit the following website: *http://www.commoncriteriaportal.org.*

An interesting trend is that more users within the community are recognizing the value of security testing, especially as it applies to accreditation decisions. The Common Criteria was always reliant on the security product user understanding the environment in which the product would be employed. For evaluation results to be used properly, one must examine the Security Target and the Validation Report, which for US evaluations, is posted on the CCEVS Web site. Although the CC evaluation provides significant insight into the security posture and the validation of vendor claims, some product vendors have begun asking Booz Allen Hamilton for testing that can be submitted as evidence for accreditation decisions efforts to facilitate receipt of an authority to operate (ATO). In these cases, we do not perform CC testing but may issue a security assessment report that not only provides senior managers and system owners with information about security vulnerabilities and associated risks present on the product or system but also helps them allocate resources to implement safeguards for reducing the overall system security risk posture.

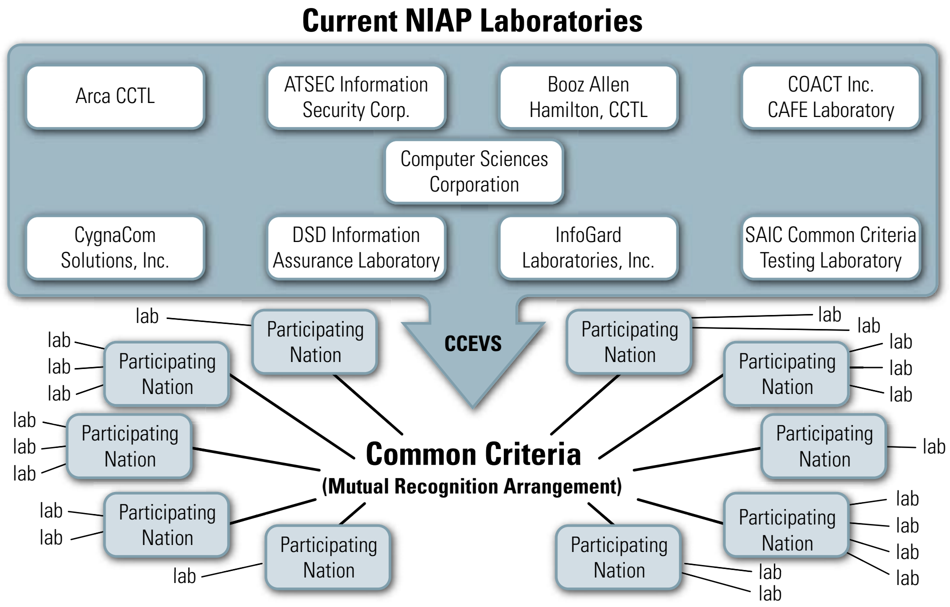

Current NIAP Laboratories
Arca CCTL
ATSEC Information Security Corp.
Booz Allen Hamilton, CCTL
COACT Inc. CAFE Laboratory
Computer Sciences Corporation
CygnaCom Solutions, Inc.
DSD Information Assurance Laboratory
InfoGard Laboratories, Inc.
SAIC Common Criteria Testing Laboratory
CCEVS
Participating Nation
lab
Common Criteria
(Mutual Recognition Arrangement)

Figure 2 Current NIAP Laboratories

As threats to our systems evolve, the CC and its implementation will need to continuously adapt to serve users. The CC Development Board meets semiannually to further develop the CC standard. The US CC Scheme also develops and distributes new policies to enhance the value of CC evaluations for vendors and customers. The goal is to continually reduce the vulnerabilities to products in use.

You can stay current on the latest policies for the US Scheme at the CCEVS website: *http://www.niap-ccevs.org/cc-scheme.*

What's Next

Users throughout the private and public sector have a need to understand more about products used in their systems and how to reduce overall risk associated with vulnerabilities introduced by those products. The CC and associated testing provide some of that information, but it must be a part of an overall system evaluation. Consumers will continue to ask more about system components, and the CC will likely evolve to meet that demand. The best minds in industry and the Government will continue to discuss and shape the future of product evaluations. ■

References

1. Capitol College. *http://www.capitol-college.edu/aboutcapitol/index.shtml.*

▷▷ *continued on page 29*

Capitol College

by Angela Orebaugh

Founded in 1927, Capitol College is a private nonprofit institution that offers BA and MA degrees as well as professional development training and certificates. The 52-acre campus, located in Laurel, MD, is dedicated to engineering, computer science, information technology, and business. All graduate-level degrees are available online and are supported by software that delivers live, real-time lectures. Capitol College prepares students for challenging, competitive careers by blending academic excellence with practical learning experiences though collaboration with business and government agencies, such as the National Aeronautics and Space Administration (NASA)-supported Space Operations Institute, National Security Agency (NSA), and Department of Homeland Security (DHS). In addition, Capitol's faculty members are scholarly practitioners who are recognized in their fields and well-connected to the industry. [1]

Capitol College offers both a BA and an MA in information assurance. Courses in the Bachelor of Science in Information Assurance (BSIA) map to the seven domains of the Systems Security Certified Professional (SSCP) certification and prepare students for the CompTIA Security+ examination. [2] The Master of Science in Information Assurance (MSIA) includes a core curriculum with elective courses in specialty focus areas. MSIA graduates prepare for careers as information systems security officers, information security analysts, administrators and consultants, risk managers and auditors, chief technical officers, chief information officers, and many more. The MSIA provides students with the professional competencies specified by the joint NSA and DHS Committee on National Security Standards (CNSS) and the (ISC)2 organization's requirements for the Certified Information Systems Security Professional (CISSP) credential. [3] NSA and DHS have designated Capitol College as a National Center of Academic Excellence in Information Assurance Education (CAE/IAE). Capitol's graduate curriculum in information assurance is mapped to the six CNSS standards, including the three standards at the advanced level. In addition to complying with the CNSS requirements, the eight required courses are mapped to all ten of the CISSP domains. [4]

Capitol College's Critical Infrastructures and Cyber Protection Center (CICPC) provides education, training, certification, research, and outreach focused on the nation's critical and cyber infrastructures. The CICPC collaborates with government, industry, and other academic institutions to address legal, technology, and policy change issues in critical infrastructure protection and cyber security.

In March 2008, Capitol College hosted "America on the Cyber Edge: A National Symposium for Pulling Together Silos of Excellence in Information Assurance." The event was a step in the right direction for addressing cyber security in the United States. The intent of the symposium was to create a dialogue and use academia as a middle ground to discuss the nation's preparedness to deter, detect, and respond to a cyber attack. The symposium characterized the nation's current state of preparedness as silos—silos of opinions, silos of expertise, silos of varying responsibilities, and silos of planning. The result is no coalesced action. A call to action was proposed to urge officials to sign pledges indicating their commitment to protecting the United States's information infrastructure. [5]

Capitol College continues to gain recognition for its academic reputation and research. The national editorial review team at *http://GetEducated.com*, an independent, online degree clearinghouse, has designated Capitol College's MS degree in computer science a "Best Buy" for 2008. The list also ranked Capitol's MS in information assurance as an honorable mention candidate. In addition, Capitol received a grant for three new scholarships under the Department of Defense (DoD) Information Assurance Scholarship program (IASP). Programs like IASP assist Capitol in its efforts to continue to produce information assurance professionals equipped to ensure the security of the nation's critical infrastructures. ■

References

1. Capitol College. *http://www.capitol-college.edu/aboutcapitol/index.shtml.*
2. BS in Information Assurance. *http://www.capitol-college.edu/academicprograms/undergraduateprograms/bsiae/index.shtml.*
3. MS in Information Assurance. *http://www.capitol-college.edu/academicprograms/graduateprograms/msiae/index.shtml.*
4. Professional Competencies. *http://www.capitol-college.edu/academicprograms/graduateprograms/msiae/competencies.shtml.*
5. National Symposium. *http://www.capitol-college.edu/newsevents/8920_228.shtml.*

DoD EWIA/CND ESSG Technical Advisory Group (TAG)

by Tarah Busbice

In previous editions of the *IAnewsletter* (Vol. 8 No. 3, Winter 2005/2006 and Vol. 9 No. 3, Fall 2006) Mr. Wayne Wise and Mr. John Palumbo of the United States Strategic Command (USSTRATCOM) described the structure and status of the Department of Defense (DoD) Enterprise-Wide Information Assurance (IA)/ Computer Network Defense (CND) Solutions Steering Group (ESSG) and its efforts. This entry will explain the structure and status of a key sub-element of the ESSG, the DoD Enterprise-Wide IA/CND ESSG Technical Advisory Group (TAG).

Mission

The TAG exists to provide technical advice to the ESSG and to provide technical requirements for solutions to be procured and implemented in support of ESSG priorities. To do this, the TAG performs seven basic activities—

1. Provides initial requirements for inclusion in a Request for Information (RFI)
2. Evaluates responses to RFIs to refine requirements for a Request for Proposal (RFP)
3. Holds Industry Days (which usually last several days) to view demonstrations from selected vendors and to further refine requirements for an RFP
4. Makes recommendations to the ESSG for each product category as to whether or not the market space is mature enough to hold a competitive acquisition
5. Staffs functional requirements through all 12 voting Combatant Commands (COCOM), services, and agencies (CC/S/A) before the release of an RFI
6. Provides requirements to the Defense Information Systems Agency's (DISA) IA/NetOps Program Executive Office (PEO-IAN) for inclusion in the RFP
7. Prepares Solutions Definition Documents (SDD) for use by PEO-IAN's Acquisition Activity.

Membership

The TAG is chaired by Tarah Busbice, Director of the Applied Technology Unit (ATU) of the Joint Task Force—Global Network Operations (JTF-GNO). Like the ESSG, the TAG consists of 12 voting organizations casting 11 co-equal votes (USSTRATCOM and JTF-GNO share a vote). Every organization within DoD should be able to find its TAG representation in the scope of each of these 12 members. Per the TAG Charter, the TAG membership list is as follows—

- USSTRATCOM
- JTF-GNO
- Defense-Wide Information Assurance Program (DIAP)
- DISA (representing DoD agencies and activities not otherwise represented in this membership list)
- United States Joint Forces Command (USJFCOM)
- National Security Agency (NSA)
- Defense Intelligence Agency (DIA) (representing intelligence community members not otherwise represented in this membership list)
- Joint Staff J6 (C4 Systems, representing COCOMs other than USSTRATCOM and USJFCOM)
- United States Air Force
- United States Navy
- United States Army
- United States Marine Corps.

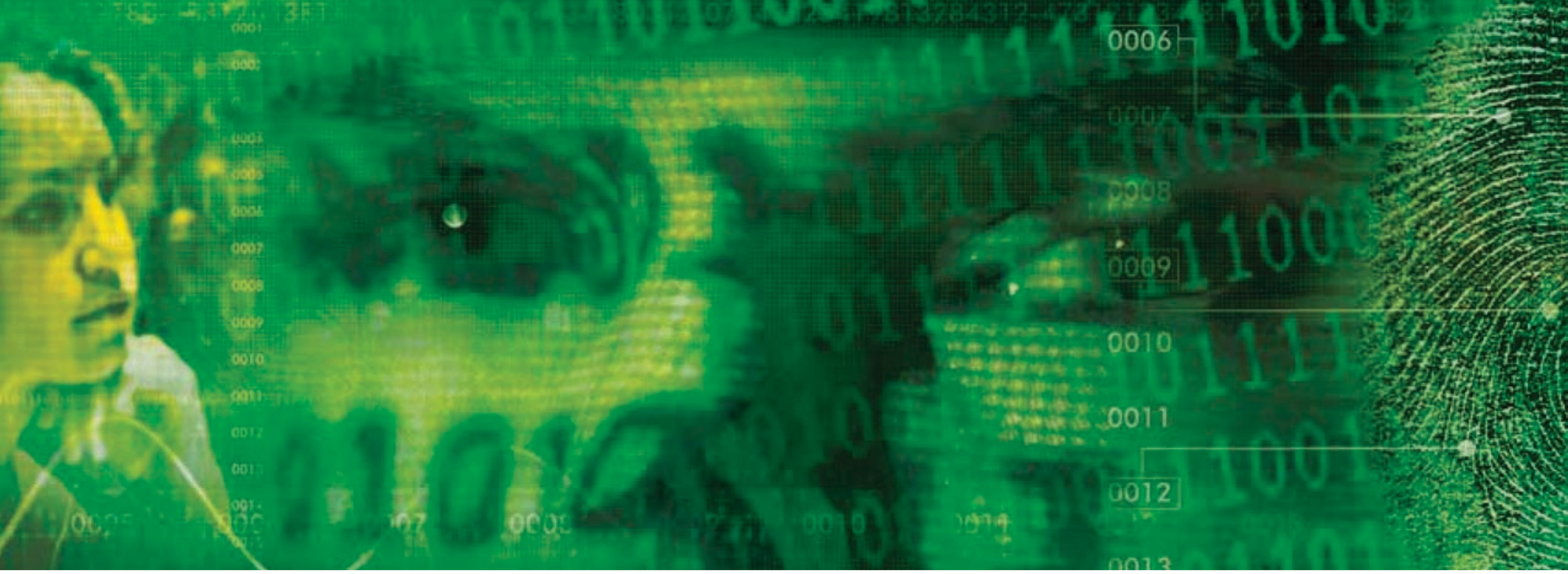
Peer Organizations

In addition to its responsibilities to the ESSG, the TAG supports peer organizations in the ESSG structure. These peer organizations include the following—

- Acquisition Working Group (AWG)
- Concept of Operations (CONOPS) Working Group (CWG)
- CND Architecture Working Group (CAWG).

Accomplishments

In the past 4 years, the TAG has performed its seven basic activities (listed above) to assist in the evaluation and acquisition of products for the following DoD Enterprise-Wide IA/CND programs—



- **Secure Configuration Compliance Validation Initiative (SCCVI)**—eEYE Retina Scanner and Remote Enterprise Manager (REM) Security Management Console
- **Secure Configuration Remediation Initiative (SCRI)**—Citadel (now McAfee) Hercules (SCCVI and SCRI are referred to jointly as the Secure Configuration Tool Suite [SCTS])
- **Spyware Detection and Eradication Program (SDEP)**—e-Trust PestPatrol
- **Host-Based Security System (HBSS)**—ePolicy Orchestrator/ Management Agent (MA)/Host Intrusion Prevention System (HIPS)/ System Compliance Profiler (SCP)/ Rogue System Detection (RSD)
- **Insider Threat Focused Observation Tool (IntFOT)**—Oakley InnerView
- **Wireless Detection Device (WDD)**—Naval Research Lab's Flying Squirrel Application
- **Wireless Mapping System (WMS)**—Naval Research Lab's Woodchuck Application (which is being bundled with Flying Squirrel).

Future Taskings

The TAG is currently performing its seven basic activities to assist in the evaluation and acquisition of products for the following DoD Enterprise-Wide IA/CND programs—

- **Insider Threat Detect (InTDET)**—The InTDET solution will correlate, analyze, and enhance existing capabilities. These include—
  - Host-based policy violations
  - Host-based behavior profiling
  - Host- and network-based trend analysis
  - Behavior profiling at the network level
  - Printer monitoring
  - Significant false-positive reduction capabilities
- **Technical Media Analysis Tool (TMAT)**—TMAT will provide DoD with an enterprise-wide capability to quickly and accurately determine the extent of a network attack and attribute that attack back to its source
- **Secret Internet Protocol Router Network (SIPRNet) Network Access Control (NAC)**—SIPRNet NAC is primarily aimed at providing device authentication on SIPRNet. SIPRNet NAC will also pursue policy enforcement and remediation capabilities on SIPRNet
- **Wireless Intrusion Detection System (WIDS)**—This program is self-explanatory
- **Host-Based Security System (HBSS) New Capabilities**—The HBSS New Capabilities Team is currently pursuing a Configuration Compliance Module, Rootkit Detection, and Data Loss Prevention capabilities
- **Secure Configuration Compliance Validation Initiative (SCCVI) Recompete**—This program is self-explanatory
- **Secure Configuration Remediation Initiative (SCRI) Recompete**—This program is self-explanatory.

TAG Week

The TAG meets monthly for the better part of a week in an event known as TAG Week. Each future tasking, determined by the ESSG as necessary to move forward, is chartered by the TAG as a sub-TAG Team, which reports directly to the TAG Chair. Each sub-TAG Team meets during TAG Week (usually for 4 hours per team). After each sub-TAG Team has met, each Team Leader provides a brief to the primary representatives of the TAG (referred to informally as the Full TAG) on its accomplishments. Whenever possible, the Full TAG meeting ends mid-Thursday, thus giving traveling Full TAG and sub-TAG Team members the ability to avoid Saturday travel. The following sub-TAG Teams presently meet during TAG Week—

- WIDS sub-TAG Team
- HBSS New Capabilities sub-TAG Team
- TMAT sub-TAG Team
- SIPRNet NAC sub-TAG Team.

▷▷ *continued on page 30*

So You Say You Want a Penetration Test...

by Casey Priester, CISSP, CISA, CEH, SSCP

Penetration testing has been a part of information security since the early 1990s, yet it is still very much a misunderstood practice—many consider it something of a "black art." Many chief information officers (CIO) and information security officers (ISO) become excited at the thought of hiring a firm to perform a penetration test because they imagine that the very act of commissioning one validates the idea that they and their organization are serious about security. This notion, combined with a lack of understanding of penetration testing realities and misconceptions about what penetration testing entails, tends to distort expectations about the penetration testing process, means, and results.

In practice, there are a number of very real, very important considerations concerning scope, risk, and goals that any organization who wishes to commission, engage in, or conduct penetration testing must carefully evaluate.

Definition of Penetration Testing

Time after time, organizations contact security firms to "do a pen test" but insist the testing be done under tightly constrained conditions and with highly structured rules of engagement, thereby defeating the purpose of the exercise.

Therefore, it is important to establish some nomenclature. What is the definition of "penetration testing"? The National Institute of Standards and Technology Special Publication 800-42 (NIST SP 800-42), Guidelines on Network Security Testing, defines it as—

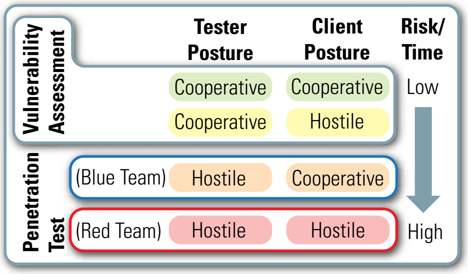
"…Security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation…to identify methods of gaining access to a system…"

"Penetration test" is an oft-abused term and should not be confused with "vulnerability assessment." The goal of a vulnerability assessment is to determine the level of risk and exposure an organization presents on external and internal networks, devices, and hosts. In a vulnerability assessment, risk is highly managed and impact to production systems is taken very seriously. Any possible negative impacts are factored in as an audit risk.

The goal of a penetration test is to break into stuff. To do so, the testers must pose temporarily as bad actors and assume a hostile attack posture to properly simulate real-world attack scenarios. Truly bad actors are not constrained by client requirements, uptime issues, or proper authorization. Although responsible pen testers take pains to avoid any intentional negative impact while posing as bad actors, the attack toolset and techniques necessarily become more direct, and the risk of negative impact rises. As NIST SP 800-42 goes on to say—

"Penetration testing should be performed after careful consideration, notification, and planning…is a very labor-intensive activity and requires great expertise to minimize the risk to targeted systems…the possibility exists that systems may be damaged in the course of penetration testing and may be rendered inoperable…Although this risk is mitigated by the use of experienced penetration testers, it can never be fully eliminated."

Below is a general illustration of the types of security testing an organization can undertake—



		Tester Posture	Client Posture	Risk/ Time
Vulnerability Assessment		Cooperative	Cooperative	Low
		Cooperative	Hostile	
Penetration Test	(Blue Team)	Hostile	Cooperative	
	(Red Team)	Hostile	Hostile	High

The vast majority of vulnerability assessments fall into the top category, Cooperative-Cooperative, with some elements of Cooperative-Hostile. These engagements usually employ industry-standard vulnerability scanning tools and data collection utilities, which are largely passive and operated under controlled conditions. In these scenarios, the rules of engagement tend to be very well defined, the audit risk is manageable, and the overall impact is generally low.

Penetration testing normally falls into the bottom two categories, where the testers assume a hostile posture and utilize a larger and more "unfriendly"

toolset, up to and including denial-of-service tools. Some of the techniques utilized by competent pen testers are large-scale packet manipulation, Layer 2 protocol manipulation, buffer overflows, SQL injection, social engineering, and other techniques largely considered hacker activities. These practices carry an element of risk that may not be suitable for certain organizations.

Black Box Testing

"Black box" testing, also referred to as "zero knowledge" testing, is a scenario in which a penetration tester operates with only the barest minimum of information about the target organization, such as a Web site or domain name. A common request is that penetration testers perform black box or zero knowledge testing on a network, operating under the assumption that to fully simulate real-world conditions, testers should operate in the same environment and with the same constraints on information that potential attackers would face. The flaw in this assumption is that the pentesters can operate with the same lack of legal restraint that actual attackers operate under.

In practice, a potential attacker has virtually unlimited time to do research, reconnaissance, and data gathering on a target network. When pen testing an organization with zero knowledge, forming a definitive picture of all available networks and services an organization may employ could take months of concerted effort. In addition, because of the nature of the tools and techniques used in penetration testing, there are further legal ramifications to consider; for example, if the testers incorrectly identify a target host or network as belonging to the client, the testers could be held legally liable for negative impact on those targets.

In addition, attackers are not constrained by the practicality or legality of other, less technology-oriented information-gathering methods, such as dumpster diving, spear-phishing, pretexting, or theft. Knowing that the human element is often the weakest link in security, determined attackers employ a wide range of clandestine or social engineering attacks to gain information. In extreme cases, they may attempt to gain physical access to a property for the purposes of theft or network backdooring. These common tools in an attacker's repertoire are not usually available or practical for penetration testing engagements. If this type of activity is requested or required, the testers would need to research and acquire sufficient legal protections for all parties and allocate sufficient time in which to carry out these activities, thereby incurring substantially greater cost to the client. For these reasons, black box testing is usually not a cost-effective measure when performing a pen test of an organization.

"Gray box" or "partial disclosure" testing is the most common type of penetration testing—and the most recommended—because it more accurately simulates a real-world scenario; that is, the pentesters are provided the type and quality of information a knowledgable attacker would be able to eventually obtain via DNS, whois lookups, search engines, SEC filings, minor social engineering, and network reconnaissance. Usually, this is as simple as providing the tester with the exact netblocks and domain names owned by the organization.

"White box" or "full disclosure" testing provides testers with complete knowledge of the hosts, networks, applications, ports, protocols, and source code to be tested. This is the most cost-effective approach for penetration testing because it eliminates all discovery, enumeration, and footprinting requirements for the testers. There are some risks to this type of testing, however. First, it does not simulate reality in any way—if an attacker ever obtained this level of detail about your organization, you would have bigger problems. Second, having full knowledge of every aspect of a system fundamentally changes the way a tester may approach attacking the system, which may run counter to the intent of the exercise, which is to simulate an attacker. Finally, if any penetration testing firm insists on full disclosure to carry out a penetration test, you should review that firm's qualifications very carefully—it may not possess the requisite skills to do a proper penetration test. White box penetration testing is best used as a follow up to black or gray box testing.

Secondary Exploitation

A central consideration of penetration testing is the depth of penetration and level of secondary exploitation desired. Some organizations may request that testers immediately cease operations as soon as verifiable compromise occurs. Others may not be satisfied if the testers compromise the entire demilitarized zone (DMZ)—they require a full assessment of how deep a determined attacker can penetrate an organization.

If full compromise and deep network penetration are desired, testers will often employ rootkits, agent-based tools, and other malware on compromised hosts in an attempt to gather information and create a base from which to deploy attacks. These tools will often remain active for weeks to maximize information gathering and to test network protections and security practices. The presence of these tools increases the risk of operational impact to the compromised hosts.

Stealth Attacks

Penetration testers are sometimes asked to attempt to evade detection or to engage a vigilant target. There are excellent business justifications for this approach, chief of which is to determine the abilities of an organization to detect, identify, and appropriately respond to intrusion attempts on the production network. However, this is not the most cost-effective approach. Several techniques for "flying under the radar" exist, and they are largely time based. Therefore, it may take days or weeks for testers to perform what would normally take hours, which can increase the cost of the effort substantially.

Successful intrusions into organizations with properly funded, trained, prepared, and alert staff are extremely improbable and exceedingly rare. The net result of such an exercise is better viewed as a "live fire" training exercise or an operational evaluation opportunity rather than a true test of organizational information security—most successful full-scale intrusions occur when vigilance is low or nonexistent.

Social Engineering

Another common request for pen-testing firms is that they attempt some social engineering attacks on the target organization. Social engineering comes with a high degree of risk not only for the target organization but also for the penetration testers themselves. Securing the proper authorizations and legal waivers before engaging in these activities is critical, and coordination with human resources, legal departments, security organizations, and even local law enforcement may be necessary to adequately ensure against liability or harm.

That being said, social engineering as a part of a penetration test has some value because it can help an organization evaluate the efficacy of security awareness training or test employee adherence to standards of conduct. It can help reveal poor security practices, policy gaps, or low security vigilance. As discussed above, the human element is often the weakest link in the security chain, and attackers take great advantage of this inadequacy.

These tests of the "human element" can be as simple as interviewing employees about security practices or posing as a vendor to solicit information about specific hardware or software used in the enterprise. They can involve other, more risky activities, such as posing as an employee to gain passwords or remote access; "dumpster diving" to determine whether sensitive data is being improperly disposed; attempting to tailgate employees into secured areas; and hijacking radio frequency (RF) access cards. Not all penetration testing firms will offer these services, and some methods verge on the exotic. Some methods cross into the realm of physical security testing. However, attackers make no such distinction. They will use any and all methods to gain access to a desired target network or system.

If requesting social engineering services as part of a penetration test, it is necessary to be very specific about the activities desired and to adequately gauge the impact these tests may have on the organization's networks, systems, and, most importantly, personnel. Employees who are successfully "duped" by a social engineer may react negatively, and organizations must take care to address the fallout from social engineering activities.

Relative Perceived Value

Most organizations value IT assets based on their own internal calculations of the asset's value and often allocate security protections accordingly—high-value systems are usually more heavily protected than low-value systems. However, attackers rarely, if ever, know the organization's valuation of that system. The majority of attackers value systems based on some combination of the available attack toolkit, their skill/preference of attack type, and the level of exploitability of the host. They discover systems using bulk scanning tools designed to search the Internet for specific vulnerabilities, and then they seek to exploit them. Even if they know that a specific system is of high ultimate value (such as an online accounting system), they may find it unbreakable—but they will look for other vulnerable systems on the same network which they can penetrate, establish a "beach head" on, and use to attack the high value system from within. Attackers understand intuitively that if the front door is locked, the side window may not be, and once they are past your perimeter defenses, they can take a detailed look at what is behind them and reassess target values.

Relative Perceived Value is the difference between the perceived value to an organization of a protected asset and the perceived value of that asset to a rational attacker. If the Relative Perceived Value is heavily skewed towards the attacker, the more time and resources will be brought to bear on it, and the chance the asset will be compromised rises. This concept can have a major impact on the ultimate efficacy of a penetration test. In an effort to reduce costs, an organization may seek to limit the scope of a penetration test to a single system or a small group of systems. Because of how attackers generally apply value to systems, the effort may ultimately fail to give an accurate representation of the overall security of the system. The system may be externally impenetrable but within reach of other, less secure systems.

Therefore, it is important to test not only the system but also its full operational context. Relative Perceived Value is important to a penetration test in that it helps better define the scope, thrust, and intent of the effort. Penetration testers understand what attracts attackers from both a strategic perspective (in terms of using it as a "beachhead" from which they can launch further attacks) and an absolute perspective (in terms of the value of the data or function of the target). By working with the penetration testers to set the testing plan and overall agenda based on this understanding, the overall value of the effort greatly increases. In addition, the organization can gain valuable knowledge on how to approach future security initiatives.

Negative Results

The vast majority of all successful network incursions occur as a result of poor configuration, known vulnerabilities left uncorrected, or the unwitting infection of an internal host by a user—not by a zero-day vulnerability or hacker über-tool. In a security-conscious organization that pays proper attention to detail, the attack surface is exceedingly narrow. In addition, as the baseline level of security applied to devices, firmware, and protocols increases, entire classes of attacks become useless. For example, at one time it was a trivial exercise to knock network devices offline simply by port scanning them or sending them bad packets, in which case they would often "fail open." As a result, there will be cases in which testers are simply unable to penetrate the network. This does not mean the exercise was a waste of money—a properly documented pen test can give very valuable information confirming the efficacy of existing controls. Nor is it a guarantee of perfect security. Attackers are opportunistic by nature; they tend to go after the "low-hanging fruit" and are constantly developing and employing new exploits and tools, often within hours of a vendor patch release. As new attacks develop, and as changes—however small—occur in the organizational network, the security posture changes. Today's impenetrable network is tomorrow's botnet; it only takes a single vulnerability.

Penetration testing is not for every organization. It carries a moderate to high level of audit risk and can be expensive and time consuming. However, performed properly and with a full understanding of both the risks and the benefits, it can impart great value to an organization's security posture and practices. ■

References

1. A hostile-cooperative effort is known as Blue Teaming, and a hostile-hostile is known as Red Teaming. For more details on this, as well as penetration testing techniques, see National Institute of Standards and Technology Special Publication 800-42 (NIST SP 800-42) at *http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf.*

About the Author

Casey Priester, CISSP, CISA, CEH, SSCP | is a Director of Operations for Prometheus Group, a full service information security firm in Chantilly, VA. He has been performing penetration testing and vulnerability assessments on commercial, municipal, and federal networks since 2001. He may be reached by email at *casey.priester@prometheus-group.com.*

▷ *continued from page 22*

COMMON CRITERIA TESTING

2. BS in Information Assurance. *http://www.capitol-college.edu/academicprograms/undergraduateprograms/bsiae/index.shtml.*
3. MS in Information Assurance. *http://www.capitol-college.edu/academicprograms/graduateprograms/msiae/index.shtml.*
4. Professional Competencies. *http://www.capitol-college.edu/academicprograms/graduateprograms/msiae/competencies.shtml.*
5. Critical Infrastructures and Cyber Protection Center. *http://www.capitol-college.edu/cicpc/index.shtml.*
6. National Symposium. *http://www.capitol-college.edu/newsevents/8920_228.shtml.*
7. Department of Defense Scholarships. *http://www.capitol-college.edu/newsevents/8920_235.shtml.*

About the Author

Steve Rome | is an analyst providing support to the CCTL. Previously, he helped NSA create and vet protection profiles, as well as the Information Assurance Technical Framework and companion Forum, while serving as IATFF Chair and Chief of the IA Solution Development and Deployment's Architectural Engineering Division. He received his BS degree in Mechanical Engineering from the University of Maryland, MBA from Central Michigan University in Management and Supervision, and an MS degree in National Resource strategy from the Industrial College of Armed Forces, National Defense University. He may be reached at *iatac@dtic.mil*

▷ continued from page 25

Voting representation for each sub-TAG Team mirrors the voting membership of the Full TAG. The primary representative to the TAG from each voting member organization appoints the voting member for his or her organization on each sub-TAG Team. In addition to the appointed members, other organizations voluntarily send non-voting representatives to sub-TAG Team meetings and Full TAG meetings.

In addition to the sub-TAG Team meetings, an activity not reporting to the TAG holds its meetings during TAG Week. This activity is the CND User-Defined Operational Picture (UDOP) Requirements Approval Board (RAB), which reports directly to the ESSG.

Decisionmaking Process

To the maximum extent possible, the TAG strives for consensus from all attendees on all decisions at TAG meetings. When consensus is not possible, the TAG requires a 60% supermajority vote of its 11 voting members (7 votes) to reach a binding decision (again, USSTRATCOM and JTF-GNO share a vote).

Additional ESSG Activities

Although the TAG supports numerous ESSG initiatives, a number of ESSG efforts do not fall under the TAG. Instead, these initiatives report directly to the ESSG. Among the efforts managed directly by the ESSG without TAG involvement are the following—

- CND UDOP
- Enterprise Sensor Grid (ESG)
- Web Content Filtering
- Anti-Virus (AV) Acquisition
- Federal Desktop Core Configuration (FDCC)
- DoD Intranet Demilitarized Zones (DMZ)
- DoD Ports, Protocols, and Services (PPS) Management Process
- SIPRNet Firewalls
- Tier 1 and Tier 2 Security Information Manager (SIM)
- Non-Secure Internet Protocol Router Network (NIPRNet)/ Internet Gateways
- Enterprise Certification and Accreditation (C&A)—Enterprise Mission Assurance Support System (EMASS). ■

About the Author

Tarah Busbice | serves as the Director of the ATU at the JTF-GNO and chairs the TAG. She has previously served as the IA Officer at the Defense Information Technology Contracting Organization (DITCO). Tarah has earned an MS in Telecommunication Management from Golden Gate University and an MBA from University of Louisiana at Monroe. She may be reached at *tarah.busbice@jtfgno.mil*

Letter to the Editor

Q ***I am interested in seeing a specific topic in the* IAnewsletter*, how do I go about that?***

A If you are receiving this newsletter, you should already be aware that this is a free quarterly publication. Our intent with the *IAnewsletter* is to feature timely and interesting articles from across the information assurance (IA) community. If you are interested in seeing us cover a specific topic, there are essentially two methods to go about doing this. The first method is to author an article on the topic. You can find article submission instructions on our website, along with all past editions of *IAnewsletter*, at *http://iac.dtic.mil/iatac/IA_newsletter.jsp*

If you are not interested in authoring an article, you can send your suggestions directly to the Information Assurance Technology Analysis Center (IATAC). We often solicit articles from across Department of Defense (DoD) organizations and from our subject matter experts (SME). We cannot guarantee that we will publish an article, but we are always looking for new and innovative ideas.

If you have any questions or concerns or are interested in proposing a topic, please email us 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 (soft copy only)

□ Firewalls □ Intrusion Detection □ Vulnerability Analysis

Critical Review and Technology Assessment (CR/TA) Reports

□ Biometrics (soft copy only) □ Configuration Management □ Defense in Depth (soft copy only)
□ Data Mining (soft copy only) □ IA Metrics (soft copy only) □ Network Centric Warfare (soft copy only)
□ Wireless Wide Area Network (WWAN) Security □ Exploring Biotechnology (soft copy only)
□ Computer Forensics* (soft copy only. DTIC user code MUST be supplied before these reports will be shipped)

State-of-the-Art Reports (SOARs)

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

UNLIMITED DISTRIBUTION

IAnewsletters Hard copies are available to order. The list below represents current stock.
Soft copy 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	

Fax completed form to IATAC at 703/984-0773

Calendar

October

TechNet Europe 2008
15–17 October 2008
Prague, Czech Republic
http://www.afcea.org/europe/events/tne/08/TNE2008Foreword.asp

Army National Guard IV-VII Logistics Management Conference
21–23 October 2008
Las Vegas, NV
https://www.technologyforums.com/8NR

DoD & IC Partnership Conference
27–30 October 2008
Dallas, TX
http://ncsi.com/dodic08/index.shtml

November

Unmanned Aerial Vehicles 2008
3–5 November 2008
London, United Kingdom
http://smi-online.co.uk/events/overview.asp?is=1&ref=2906

Unmanned Aerial Vehicles 2008
5–6 November 2008
Chicago, IL
http://infosecurityconference.techtarget.com/conference

Unmanned Aerial Vehicles 2008
17–18 November 2008
London, United Kingdom
http://smi-online.co.uk/events/overview.asp?is=1&ref=2994

December

Defense Network Centric Operations 2008
1–3 December 2008
Arlington, VA
http://www.wbresearch.com/DNCO/?cm_mmc=affiliate-_-listing-_-11357.002_-_zevents

Air Force IT Day
3 December 2008
McLean, VA
http://www.afcea.org/calendar/eventdet.jsp?event_id=16470&w=Y

CyberSpace/CyberWarfare
10–11 December 2008
Washington, DC
http://www.afcea.org/events/register.cfm?ev=19

February

Information Assurance Symposium
3–6 February 2008
Dallas, TX

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