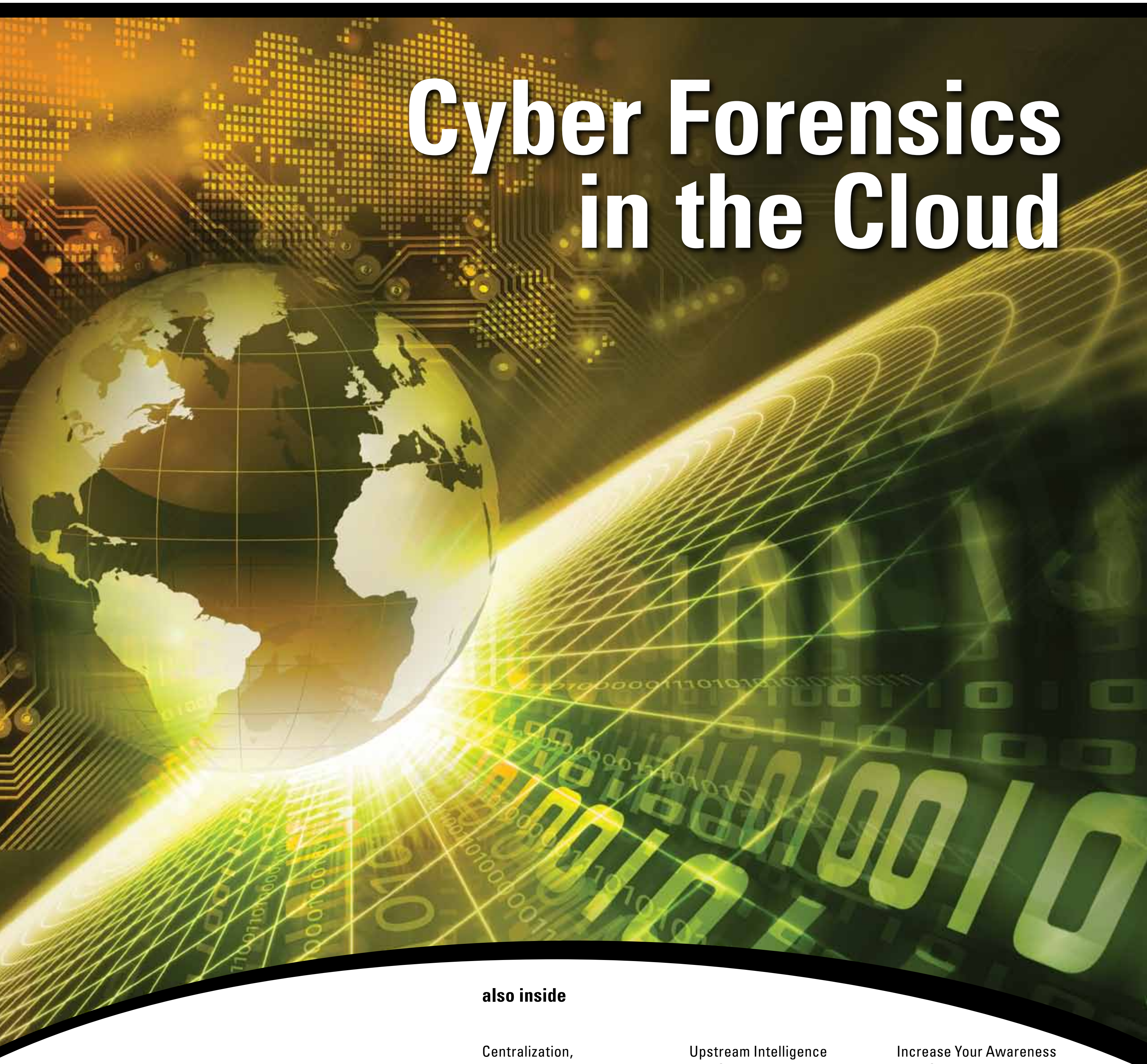
14/1

IAnewsletter

Volume 14 Number 1 • **Winter 2011**

The Newsletter for Information Assurance Technology Professionals



Cyber Forensics in the Cloud

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 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: Ryan Skousen

If you are interested in contacting an author directly, please e-mail us at *Iatac@dtic.mil.*

***IAnewsletter* Staff**
Chief Editor: Gene Tyler
Assistant Editor: Kristin Evans
Art Director: Lacey Olivares
Copy Editor: Daniel Eckroad
Barbara Veneri
Editorial Board: Al Arnold
Angela Orebaugh
Dr. Ronald Ritchey
Designers: Michelle DePrenger
Dustin Hurt
Kacy Littlehale
Peter Lewis
Don Rowe

***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 e-mail 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

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

Deadlines for Future Issues
Spring 2011 January 28, 2011

Cover design: Michelle DePrenger
Newsletter design: Donald Rowe

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

in every issue

IATAC Chat

Gene Tyler, IATAC Director

IATAC has enjoyed a long and close relationship with the Institute for Applied Network Security (IANS), an organization that focuses on conducting critical information assurance (IA) research for our community with a special focus on business and industry. IANS experts contribute the "Ask the Expert" column to each edition of the IAnewsletter, which provides answers and insight into some of the more vexing IA questions we all have. In the past, this column has sparked debate among some of our government authors. For example, in the Spring 2010 edition, Dr. Bret Michael and Dr. George Dinolt began their article citing former IANS expert, Allan Carey. In the Winter 2010 edition "Ask the Expert" column, Mr. Carey expressed his opinion that cloud computing security problems are almost synonymous to virtualization security problems. Dr. Michael and Dr. Dinolt went on in their article to explain how they disagreed. IANS' contributions continue to make this publication more interesting and multi-dimensional.

IANS also organizes several IA workshops throughout the year. As I mentioned in my last chat, the IANS Mid-Atlantic Information Security Forum is scheduled to take place 8-9 March 2011 at the JW Marriott in Washington, DC. Every year, this event gives each participant a seat at one of several expert-led roundtable discussions. An IA subject matter expert (SME) in a particular area begins each discussion with a brief introduction to a specific IA topic. Then that SME facilitates a focused discussion among industry, government, and academic participants who share their expertise in order to develop new IA solutions.

At last year's forum, IATAC SMEs participated by leading roundtable discussions and by presenting on different IANS focus topics. Some of the roundtable and presentation topics included: Continuous Monitoring, Cloud Computing, New Developments in Cyberlaw, Training and Awareness, and Securing Industrial Control Systems. This year's agenda is not yet finalized, but will focus on topics of interest to the government. I think IANS offers a lot for everyone, and because they bring their unique business and industry focus to the forefront, they are worthy of greater attention. I often say that, "IANS is to IA what IEEE is to engineering." I often talk with IANS' leadership to gain a better IA perspective. After participating at last year's forum, I came away with a far better understanding of the current state of IA, the problems we are facing as a community, and the direction we are heading.

Similarly, I think the collection of articles we have compiled for this edition gives our readers a taste of where our community is currently, the problems we are facing, and the solutions that will move us into the future. Scott Zimmerman and Dominick Glavach discuss how antiquated cyber forensics techniques must now adapt to meet the demands of cloud computing environments. This is a prime example of how new technology—cloud computing—has created a new challenge that we must address. To caveat this article, Kevin McLaughlin's article discusses how taking a centralized versus decentralized approach to determining an organization's security architecture can have both positive and negative effects. The current state of IA is largely determined by decisions such as whether or not an organization should take a centralized versus decentralized approach to security.

Dr. Sheela Belur presents a mathematical model that can help determine whether or not an information system architecture's design is superior to its alternatives. The IA community continuously faces the challenge of selecting what technology is best, and this article presents a method for making that determination.

In looking ahead, Tyson Macaulay finishes his seven-part series on Upstream Intelligence (UI), which quantitatively identifies information security threats. Mr. Macaulay's in-depth analysis of how we can assess threats using UI is one example of how our community is responding to meet future IA needs. On behalf of IATAC, I thank him for providing our readers with this interesting glimpse into an innovative capability that promises to propel us forward.

As always, I encourage readers to contribute articles to the *IAnewsletter.* I also encourage you to visit our Web site for more information on our IA products and services. I hope the information IATAC provides the IA community helps us all meet future IA challenges together.

Gene Tyler

*For more information about the **IA Symposium** and the **2011 Identity and Information Assurance Award**, see page 33.*

Cyber Forensics in the Cloud

by Scott Zimmerman and Dominick Glavach

According to research firm Gartner, cloud computing services revenue should total $68.3 billion for 2010, representing a 16.6% increase compared to 2009. The market is expected to explode to $148.8 billion in 2014. [1] This trend toward cloud computing is creating numerous challenges for cyber forensics professionals. In traditional models, an information assurance or digital forensics professional operates in a domain where system components are within physical reach and ownership boundaries are well defined. The forensic analyst works directly for an organization and has access to—if not directly administers—the organization's computing infrastructure. An organization's network infrastructure has uniform configurations and settings that they can collect, preserve, or analyze. For example, date stamps are consistently applied, and memory allocation and overwrite procedures are clearly and evenly executed. These consistent system configurations and behaviors (or breaches of anticipated behaviors) are an integral component of a forensic investigation. In a cloud model, consistently configured network infrastructure becomes less consistent. For example, because user systems and cloud systems can be separately administered, date stamp settings may differ from the user side and the provider side where the requested application lives in a cloud. How then can a digital forensics professional match up a user request to an actual use time?

This article addresses a variety of technical issues concerning cyber forensics in the cloud. But first, some definitions are in order.

Cloud Computing

Cloud computing is an emerging model that separates application and information resources from the underlying infrastructure, and the mechanisms used to deliver them. The National Institute of Standards and Technology (NIST) defines cloud computing as "…a *model* for enabling convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.,* networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [2]

Cloud computing is not a new technology but a new way of providing computing resources and applications on demand. These resources are varied but generally fit into one of the three service delivery models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The opportunities and challenges associated with each of these three is discussed later in this article.

Key Benefits of the Cloud and Associated Cyber Forensic Challenges

There are two key benefits of the cloud delivery model:

- **Cost savings—**Users pay only for the computing resources (*i.e.,* applications, memory, *etc.*) as needed and on demand. This pay-as-you-need model is analogous to the consumption of electricity or water.
    - **Associated Cyber Forensic Challenge—**This elasticity poses a challenge to the forensics investigator due to resources such as disk space and memory allocated today that is gone and overwritten tomorrow.
- **Infrastructure independence—**Cloud services can be used without the need to know or understand how the underlying infrastructure operates or is physically located.
    - **Associated Cyber Forensic Challenge—**This lack of understanding makes it imperative that strong relationships and agreements are formed between your organization and the Cloud Service Provider (CSP).

There is ongoing debate as to the privacy and security that the cloud provides. One thing is certain, however; it is not a question of *if an incident will occur* but *when and how severe*. As a result, we need to proactively prepare now to execute computer and network forensics in the cloud.

To date, there has been very little research done on the current state of the tools, processes, and methodologies to obtain legally defensible digital evidence in the cloud.

Case Study

Your agency has decided to leverage the many advantages of cloud computing and wants to move several applications off of your internal intranet to an approved CSP. Your goal is to eliminate the need to continually add new hardware to your footprint. For years, every new project has required you to add new servers and communications hardware to the infrastructure, consuming more power, increasing your physical footprint, and creating nightmare management issues. On top of that, this new infrastructure is only operating at a very small portion of its capacity. The cloud looks very appealing.

After several months in the cloud, you get a phone call from your manager. She wants to know if you remember the contractor who worked in acquisition and who was terminated last month. You say you do and that you shut off all of his account access and all the files from his e-mail are stored in the usual place for terminated employees. She says thanks, but she needs all of files that he had access to including the ones from that new application your agency put into the cloud six months ago. Now what?

Problems with Traditional Digital Forensics in the Cloud

The current operational landscape of incident handling and forensic methods have changed with the evolution of cloud computing. We no longer have the ability to physically acquire objects in these virtual environments where disks, memory, and networks are shared, and traditional ownership boundaries are blurred.

To date, there has been very little research done on the current state of the tools, processes, and methodologies to obtain legally defensible digital evidence in the cloud. The Cloud Security Alliance and forensics practitioners agree that additional research needs to be done to develop a framework of methodologies and processes that will stand up in a court of law. They recommend,

> *"being able to restore systems to earlier states, and even a need to go back six to twelve months for a known-good configuration. Keeping legal options and requirements in mind, remediation may also need to support forensic recording of incident data."* [3]

What is Cloud Forensics?

Computer forensics is the art and science of applying computer science knowledge and skills to aid the legal process. [4] When acquiring digital artifacts in the cloud, whether for preservation, presentation in a court of law, or the internal investigation of employees misuse, basic forensic principles and processes apply. The forensic process is broken into four distinct steps:

- **Collection**—artifacts (both digital evidence and supporting material) that are considered of potential value are collected
- **Preservation**—preservation of original artifacts in a way that is reliable, complete, accurate, and verifiable
- **Filtering**—analysis of artifacts for the removal or inclusion of items that are considered of value
- **Presentation**—step in which evidence is presented to support investigation.

Cloud forensics applies this same forensic process but has the challenge of combining various physical and logical locations. These areas include the following:

- **Client-side—**technical controls or monitors implemented on networks and computers under client control or ownership (Intrusion Detection System [IDS], Web Content engine logging, firewalls, access log, chat logs [locally], *etc.*)
- **Combined-side—**technical controls or monitors implemented on networks and computers allocated to cloud customers (access logs, transaction logs, usage logs, *etc.*)
- **Provider-side—**technical controls or monitors implemented on networks and computers that support or comprise the cloud service (firewalls, load balancers, admin access logs, IDS, NetFlow data, *etc.*).

A challenge is to provide sufficient pure forensic data from the cloud to prove the event/action did occur. You may not be able to create a bit-by-bit copy of the evidence, but you should be able to obtain a snapshot of the existing data from the cloud and recreate access *via* logs to the cloud resource (verified by client-side NetFlow and firewall logs and provider-side firewall logs, as well as access logs on the laptop used to access the cloud resource). The current challenge is to convince other parties that this event occurred in the manner just presented. Similar approaches are being used in criminal cases where digital evidence is used as supporting documentation versus judicial evidence. The notion is that an event cannot be ignored or discounted if there is substantial supporting information that validates the claim.

Two technical challenges are location and time:

- **Location—**Before network or computer forensics can begin, the network or computer must be "found." There may only be traces of a virtual machine (VM) because the VM may reside on dispersed, internationally-located physical drives; data may have been deleted from a striped multi-disk array unit; or forensics may reside within another cloud vendor storage system that involves court orders to retrieve.
- **Time—**Once the information source is identified, do all involved entities have time synchronized *via* a consistent time source such as Network Timing Protocol (NTP)? If a forensic expert has a difficult time convincing your legal counsel that the time stamps from client-side log files match time stamps on provider-side log files, the forensics will be difficult to defend.

Tools for Performing

Current forensic tools are based on traditional forensic approaches, including formal methods to acquire information and a structured method to analyze artifacts with the intention to recreate or validate some series of events or retrieve missing information. These forensic tools fall into two general categories:

- **Static—**Static analysis forensic tools analyze stationary data, the contents of hard drives or NetFlow data, obtained through a formalized acquisition process.
- **Live—**Live forensic tools collect and analyze "live" system data, accommodating the order of volatility, performing memory analysis, and providing methods for encryption key recovery.

The two categories exist as a result of forensic evolution to recreate and document sophisticated incidents. However, cloud models break this paradigm because information is difficult to locate, acquisition is impossible when location is questionable, and analysis is nonexistent without acquisition. A third forensic tool evolution is needed to facilitate cloud forensics analysis.

Cloud forensic tools need to be a hybrid of the current static and live collection and analysis methods, and they need intelligence to note and predict artifacts based on forensic heuristics. In incidents when traditional forensic tools fit, the only aspect a cloud tool changes is the collection method. In incidents where acquisition is a challenge, next generation forensic tools must visualize the physical and logical data locations. The visualization must indicate obtainable and unobtainable artifacts, easing the collection burden and preservation estimates. Unobtainable artifacts should be annotated as such in an automated fashion, and the annotations should be evidences carried into the evidence presentation. In addition to visualization, cloud forensic tools need to use the cloud as a discovery engine for rapid and accurate forensic determinations. Forensic collections containing unobtainable artifacts should be submitted into a cloud environment for heuristic and signature based analysis. This uses a method similar to antivirus engines and other binary analysis engines as the number of submissions increase, thus allowing forensic investigators to convert incomplete collections to reliable presentations.

Cloud Forensic Opportunities and Challenges with IaaS, Saas, and PaaS

Finally, each of the three Cloud Service Models presents both their own opportunities and challenges. These are outlined in Table 1.

Conclusion

There are many technical and physical issues with performing cloud forensics that need to be researched and addressed. Some of these issues can be addressed by using current forensic tools and processes in a different manner, while other issues require that new approaches and systems be developed.

In addition to the development of new tools and systems, a strong working relationship needs to be developed with CSPs including a Service Level Agreement (SLA) to provide assurances they that are a

Cloud Computing Models	Opportunities	Challenges
IaaS	▸ Traditional forensic acquisition may apply ▸ VM snapshots can accommodate preservation letters or serve as the acquisition image(s) ▸ Designed for high availability so network access data is very likely to be present and accurate ▸ Client-side information is highly likely on the end-device or transient devices ▸ The easiest of the three models.	▸ Live forensics and access to volatile data may not be possible (some vendors may not utilize persistent storage) ▸ Storage is logical and focused on allocated space; acquisition images may not include data remnants or unallocated disk space ▸ Unobtainable failed or obsolete hardware ▸ Multi-tenant storage devices may contaminate the acquisition ▸ Logging may be co-located or spread across multiple and changing devices ▸ Acquisition may require large amounts of bandwidth to complete in a timely manner ▸ Data fragmentation and dispersal ▸ Data ownership issues—what happens when the contract is terminated?
SaaS	▸ Access to application / authentication logs are possible ▸ Client-side information is highly likely on the end-device or transient devices ▸ SaaS application features may assist with network forensics ▸ Provider-side devices contain basic access information.	▸ Traditional acquisition is highly unlikely ▸ Logging and log details depend on CSP ▸ Information may be inconsistent across application programming interfaces (API) ▸ Other CSPs may be involved ▸ CSP applications may be complex and difficult or impossible to analyze ▸ Process/application isolation ▸ Systems are more proprietary in nature.
PaaS	▸ Client-side forensics is very likely (we control the source and development cycle) ▸ Web-server or virtualized operating system (OS) forensic methods apply.	▸ Logging relies on the CSP environment (system calls may not function in CSP) ▸ Systems are more proprietary in nature.

Table 1 Cloud forensic opportunities and challenges among the cloud service delivery models.

part of your team and can collect and provide sufficient forensic artifacts when needed. ■

References

1. Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010. *http://www.gartner.com/it/page.jsp?id=1389313* (accessed November 2010).
2. The NIST Definition of Cloud Computing, Version 15, Peter Mell, Tim Grance, National Institute of Standards and Technology, *http://csrc.nist.gov/groups/SNS/cloud-computing/,* October 2009, (accessed April 2010).
3. "Security Guidance for Critical Areas of Focus in Cloud Computing," Cloud Security Alliance, December 2009, *http://www.cloudsecurityalliance.org/csaguide.pdf,* (accessed April 2010).
4. Brown, Christopher L.T. "Chapter 1 – Computer Forensics Essentials." Computer Evidence: Collection and Preservation, Second Edition. Cengage Learning. © 2010. Books24x7, *http://common.books24x7.com/book/id_33937/book.asp,* (accessed April 2010).

About the Authors

Scott Zimmerman, CISSP, ISSEP | has 27 years of information technology and cybersecurity experience and is a principal technical advisor at Concurrent Technologies Corporation (CTC) in Johnstown, PA. Mr. Zimmerman's education includes a BS in management information systems and AS in electronic/computer technology. He is a Certified Information Systems Security Professional (CISSP), Information Systems Security Engineering Professional (ISSEP), and a member of the Cloud Security Alliance. He currently serves as a technical director on several DoD/IC programs.

Dominick Glavach, CISSP, GCIH | is a principle information systems security engineer at CTC with 16 years of cybersecurity experience. He is the information security lead in CTC's enterprise infrastructure and supports CTC projects in technical and subject matter expert roles. Mr. Glavach received his BS in computer science from the Indiana University of Pennsylvania, and he maintains a CISSP, Global Information Assurance Certification (GIAC) Certified Incident Handler (GCIH), and other certifications. He is a member of the Computer Security Institute and Cloud Security Alliance.

Centralization, Decentralization and the Impact on Information Security Programs

by Kevin McLaughlin

Organizations are under constant pressure to create an environment which adequately protects the data items they have been entrusted to protect. To protect these data items, organizations need to decide on the proper security architecture to put in place. Should they use decentralized or centralized security resource architecture to safeguard their data? More importantly, should they have centralized or decentralized command and control of these resources? If centralized, they need to consider how stove-piping can be avoided or minimized. This article discusses which approach is most effective when creating an organizational security program.

Problem Statement

Few companies have adequate information security resources to accomplish their goals. Information security/assurance, referred to as information security, is responsible for incident response, vulnerability scanning, security monitoring, access controls, security awareness programs, risk management, new project security reviews, investigations, and, in some cases, physical security, mobile device security, *etc.,* within an organization. Organizational units have varied distribution, *e.g.,* finance is usually a different department with separate functional management than human resources, which makes it difficult for a centralized information security program to maintain and control all of the organizational security resources under one umbrella. This article reviews both the centralized and decentralized information security approaches and discusses taking a hybrid approach.

"The most efficient way to produce anything is to bring together under one management as many as possible of the activities needed to turn out the product." — Peter Drucker

Background and Discussion

The prevalence of identity theft and successful phishing attacks that place malware on systems to enable black hats—commonly referred to as hackers—to steal money from a victim or make use of a victim's private information without their permission has heightened the concern among computer users. [1] With the user population fluctuating and organizational communities expanding to include business partners, trusted alliance partners, suppliers, affiliates, and customers, providing adequate protection schemes for regulated data is more pressing than ever. [2]

Centralized approaches are often considered not as responsive to organizational department needs as compared to direct management and control by individual department heads. [3] An effective information security program must consider the development, maturation, and assessment of unit level adherence to information security programs. [4] Diverse business units, with various information security responsibilities requiring multiple levels of collaboration, make communication and compliance to baseline security practices difficult. [5] Owners of security resources deployed throughout the organization must accept responsibility and be accountable for how well or how poorly these resources fulfill their purpose. To avoid misunderstandings, owner responsibilities must be clearly defined and communicated. [6] Inadequate adherence to information security principles and guidelines is often the main reason attackers successfully exploit various organizational attack vectors (OAV). [7] This noncompliance often occurs because the organization lacks a centralized command and control structure to assess individual department compliance.

Resource centralization commonly uses operational strategic methodology to implement strong information security architecture. This architecture spans organizational units to lower costs, improve

efficiency, and gain better control over operational components. [8] The centralization approach is a logically deployable methodology for organizations with a data-centric philosophy: "organizations are focusing on information centric security because infrastructure is mostly static, while information is mobile." [9]

If organizations want to have adequate command and control of deployed resources, they must layer their security architecture so that their centralized security resources provide multiple cross-departmental security points. When implementing a centralized approach methodology, the department with the central command and control must not be viewed as an "ivory tower," or a place where decisions are made and distributed, but which fails to help other departments implement a good information security infrastructure. Another concern with running security resources centrally is ensuring that they do not become a single point of failure or become stove-piped. Centralizing information security resources must be managed and implemented with resilience in mind. [10]

One current centralized approach is cloud computing and the creation of centralized information technology (IT) resources in the cloud, which by extension need to be protected in the organizational cloud. [11] The concept and theory behind cloud computing drives organizations toward centralized information security command and control of the items sitting within the organization's centralized cloud. However, the emergence of this technology does not mean that autonomous knowledge worker computing developed by personal computers (PC) is no longer a valid method of implementing IT or information security work processes. [12] This is a key point to consider when making strategic decisions on what an organization's information security program should look like. As long as we have autonomous knowledge workers, we will have to design information security programs that rely to an extent on these workers to be effective. These independent workers can command and control information security resources. These workers frequently make security decisions in a vacuum without consulting their organization's information security specialists. [13] This often creates an environment where amateurs and hobbyists make critical data protection decisions and conduct security data analysis without adequate training, preventing them from making the most knowledgeable decisions.

The creation of a centralized command and control security architecture provides organizations with a strong, consistent approach, with few functional drawbacks.

In times of duress and emergency, it may be necessary to deploy and use a large number of temporarily assigned resources to recover from the emergency. These temporary resources may span the entire organization, but they should be managed and controlled centrally so that adequate focus resides on the management command structure's specific priorities. These temporarily assigned security resources must also be provided with the authority to handle the unexpected and make command decisions in the absence of the normal management structure. [14] These decisions should be deployed and implemented based on a strategic organizational information security framework. The organization should receive annual training on this framework. This model follows the federally structured emergency management program in which the local emergency managers are an autonomous part of a nationally centralized whole.

Managing information security and its associated resources is challenging. That challenge is compounded when centralized command and control is absent. [15] It is easier to establish a consistent methodology when a centralized command and control structure is in place. A centralized architecture is one of the most powerful and easy architectures to implement. [16] The creation of a centralized command and control security architecture provides organizations with a strong, consistent approach, with few functional drawbacks. Developing this centralized security resource approach also tends to increase the power of information security across the organization. Since power often "determines the capability an organizational unit has to influence the behavior of other units," a centralized environment better positions information security resources for greater success than would a decentralized environment. [17]

Information security professionals have worked with their end user community to attempt to create an atmosphere of self-regulation regarding the implementation of best practice security controls and methodologies. However, the number of reported security incidents increases annually, demonstrating the failure of decentralized self-regulation—alternative approaches need to be taken into consideration. [18]

Some information security practitioners support centralization, arguing that it promotes effective disaster recovery and business continuity programs; minimizes labor redundancies; facilitates volume purchasing discounts on security tools; and provides lower training costs through more standardized and re-applicable training. [19] Further, mobile computing devices account for more than half of all organizational information security breaches. As such, chief information officers should consider implementing a more centralized security management infrastructure for these devices. [20]

The US government learned valuable lessons from events like the terrorist attacks on 11 September 2001, demonstrating how a completely self-contained centralized approach is not effective. There is simply too much work, too many items, and too large a scope for any one centralized agency to be successful doing it on their own. This realization has led to the federal governance structure of a hybrid design consisting of "centralized infrastructure control" and decentralized control methodology, allowing for flexibility in work tasks and responsibilities. [21] This flexibility component is critical considering that organizations are "evolving social forms of sense making," and therefore will utilize diverse resources with differing ideas and techniques to implement effective security controls and processes, which tie into the centralized security pool of resources. [22]

A hybrid approach is the current method that is being promoted by US government agencies such as the Department of Homeland Security (DHS). The DHS outreach and education program trains individual local government employees (*e.g.,* emergency services) in emergency response techniques, how to work together as an integrated whole with federal agencies, and how to pass and share information across diverse local, state, and federal agencies.

Taking a Hybrid Approach

For an organization to create an effective information security environment, it must utilize a hybrid approach that contains an information security department to provide centralized resource command and control and oversee decentralized responsibilities. Swanson and Guttman acknowledge this point:

> *"Managing computer security at multiple levels brings many benefits. Each level contributes to the overall computer security program with different types of expertise, authority, and resources. In general, executive managers (such as those at the headquarters level) better understand the organization as a whole and have more authority. On the other hand, front-line managers (at the computer facility and applications level) are more familiar with the specific requirements, both technical and procedural, and problems of the systems and the users. The levels of computer security program management should be complementary; each can help the other be more effective. Many organizations have at least two levels of computer security management; the central level and the system level." [23]*

By analyzing the inadequate historical approach to information security that many higher education institutions originally took towards creating their security environment and culture, we have found that a decentralized information security command structure is ineffective. [24] Many colleges and universities spread command and control for various information security regulatory areas across multiple, non-integrated departments, such as the University Hospital—responsible for Health Insurance Portability and Accountability Act (HIPAA) compliance; the Registrar—responsible for Family Educational Rights and Privacy Act (FERPA) compliance; and the Treasurer—responsible for Gramm-Leach-Bliley Act (GLBA) compliance. [25] An effective argument can be made that only a centralized approach to information security allows an organization to fully understand and effectively integrate the disparate regulatory and legislative data protection requirements into a comprehensive compliance program. The most effective way to achieve this goal would be to centralize information security resources in a single place, so that it can be effectively managed and maintain the appropriate level of controlled trust. [26]

Organizations that follow a unified information security compliance approach will ensure an efficient and cohesive method to achieve and maintain information security protections. As mentioned above, a unified approach is effective because HIPAA, the Federal Trade Commission regulations for GLBA, 21 C.F.R. Part 11, Payment Card Industry Data Security Standards, and the laws on notice of security breach specify or suggest many of the same security risk analyses and management practices. [27]

It is insufficient to simply suggest that a centralized approach be taken when developing an effective organizational information security environment. Too many disparate and disconnected parts prevent a single department from effectively managing the detailed security items that must be established and tracked across each of the organization's departments by each individual working or affiliated with the organization.

While there must be strong, centralized command and control provided by a centralized information security office, there should also be a departmental training program to instruct each organizational resource on how to safeguard protected organizational data. Not only must there be an effective training program, there must also be an effective monitoring program to assess the organizational and individual department resources' adherence to policies, procedures, and tasks set forth by the centralized information security department. Hence, the individual organizational and affiliated staff members decentralized adherence to tasks is critical to information security infrastructure strength.

Information security training courses often use the example, "What's missing here…SEC—ITY? UR," to emphasize that effective information security can only occur once everyone is involved and knowledgeable about safeguarding organizational data.

Determining if department members are following central information security policy or decentralized monitoring is the responsibility of each of the decentralized department managers. The organization's information security program is effective only if the information security command and control department has the authority and resources to assess individual department adherence to the organization's agreed upon information security program tasks. [28]

A hybrid solution allows for strong integration and consistency for compliance with regulatory items, as well as synergistic data protection solutions that span the organization. This approach also establishes the foundation for a security resource training and security awareness program that provides a strong and consistent message and method for each organizational resource and departmental manager. This approach can be applied to all three information security communities of interest: business resources, management resources, and IT resources. ■

About the Author

Kevin McLaughlin | began his career as a special agent for the Department of the Army. He has had many careers over the years, including being a police officer in Kissimmee, FL, a middle school teacher, a director at Kennedy Space Center, the president of his own company, and an IT manager and senior information security manager with the Procter & Gamble (P&G) company. Kevin currently works at the University of Cincinnati as the assistant vice president of information security. He is responsible for all aspects of information security management, including, but not limited to, strategic planning and the architecture and design of information security solutions.

References

1. Adler, M.P., A unified approach to information security compliance. EDUCAUSE Review, 2006: p. 47–59.
2. Ahuja, J., Identity Management: A business strategy for collaborative commerce. Information Systems Control Journal, 2003. 5.
3. Brandel, M. and M. Betts, Swinging toward centralization. Computerworld, 2010: p. 16–19.
4. Montgomery, M. Unit-level computer defense in United States Naval Institute, Proceedings. 2003.
5. Bharosa, N., J. Lee, and M. Janssen, Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: Propositions from field exercises. Information Systems Frontier, 2010. 12: p. 49–65.
6. Swanson, M. and B. Guttman, National Institute of Standards and Technology. Generally accepted principles and practices for securing information technology systems, 1996: p. 1–57.
7. Srinivasan, S., Information security policies and controls for a trusted environment. Information Systems Control Journal, 2008. 2: p. 1–2.
8. Brandel and Betts, op. cit.
9. Mody, S., End users are the real security threat. McClatchy - Tribune Business News, 2008.
10. Ross, S., Information security and the resilient enterprise. Information Systems Control Journal, 2005. 2.
11. Crosman, P., Aiming for the clouds. Wall Street & Technology, 2009. 27: p. 26.
12. Robey, D. and M.C. Boudreau, Accounting for the contradictory organizational consequences of information technology: Theoretical directions and methodological implications. Information Systems Research, 1999. 10(2): p. 167–185.
13. Wood, C., An unappreciated reason why information security policies fail. Computer Fraud & Security, 2000: p. 13–14.
14. Ross, op. cit.
15. Shehab, M., A. Ghafoor, and E. Bertino, Secure Collaboration in a mediator-free distributed environment. Parallel and Distributed Systems, 2008. 19(10): p. 1338–1351.
16. Schumacher, S., How to preserve security and autonomy while meeting information-sharing directives. ISACA Journal, 2009. 6: p. 1–2.
17. Xue, Y., H. Liang, and W. Boulton, Information technology governance in information technology investment decision processes: The impact of investment characteristics, external environment, and internal context. MIS Quarterly, 2008. 32(1): p. 67–96.
18. Adler, op. cit.
19. Brandel and Betts, op. cit.
20. Nalneesh, G. and B. Kiep, Managing mobile menaces—If I.T. is everywhere, who's responsible for security threats? Here's a plan for managing some of the most unmanageable risks. Optimize, 2007. 6(5): p. 40.
21. De Haes, S. and W.V. Grambergen, IT Governance and its mechanisms. Information Systems Control Journal, 2004. 1.
22. Dhillon, G. and J. Backhouse, Risks in the use of information technology within organizations. International Journal of Information Management, 1996. 16(1): p. 65–74.
23. Swanson and Guttman, op. cit.
24. Adler, op. cit.
25. *Ibid.*
26. Byrne, J., Large-scale biometric management: A centralized, Policy-based approach to reducing organizational identity chaos. Information Systems Control Journal, 2003. 5.
27. Adler, op. cit.
28. Montgomery, op. cit.

A Figure of Merit Model for Assured Information System Architecture Design

s(Ai) = S(Ai) /Max{S(Ai), i=1
s(Ai) = S(Ai) /Max
e(Ai) = E
e(Ai) = E(Ai) / Max{ E(Ai)
s(Ai) = S
F(A_i) = W_1 s(A_i) = W_2 e(A_i) = W_3 p(
e(Ai)

by Dr. Sheela Belur

A mathematical model to estimate the figure of merit of an assured information system architecture design is proposed to aid the Analysis of Alternatives (AoA) of candidate architectures. This figure of merit function is defined as the weighted algebraic sum of the *strength* of the security mechanism, *ease of use*, *system performance*, and *cost*. The feasibility of the mathematical model is demonstrated by its application to an example architecture design, and the advantages of adopting such a quantifiable figure of merit model at the AoA of architecture design are outlined.

> When several candidate architectures are evaluated, their relative merits can be estimated only when a composite or a unified function of security strength, ease of use, performance, and cost are defined and computed.

AoA is an important step in any system architecture design. It is even more so in an information system security architecture design. While it is very important to ensure information system resources are protected and not acted upon by unauthorized users, it is important to note that there are several other factors that could influence choosing a particular architecture over another among multiple candidate architectures that meet the same functionalities. Among these factors, *ease of use*, *performance*, and *cost* stand out as the most critical. The overall *security strength* of an architecture design is a function of the various controls chosen for the architecture. If the security controls of an architecture design make functionality difficult for an end user, the chosen architecture, albeit secure, would be undesirable. Secondly, if the resulting response time for certain use cases of the system is very high, the architecture option would be relatively less attractive compared to others. Finally, *cost* is the sum total cost for the components comprising the architecture and is the sum total of the product, installation, and maintenance costs of the components over their lifetime. Therefore, when several candidate architectures are evaluated, their relative merits can be estimated only when a composite, or a unified function, of the factors above are defined and computed.

In [1], a Figure of Merit (FoM) mathematical model was presented as a multivariate function of security controls for an assured information sharing system, the problem of determining the optimal set of security countermeasures for a given system was then formulated as a mathematical optimization problem, and the potential methods of approach were addressed. In this article, the concept is extended to be applicable for the evaluation of multiple candidate architectures of an information system. Toward this end, a composite mathematical function is defined in which a linear combination of the *security strength*, *ease of use*, *performance*, and *cost* factors have coefficients corresponding to the weight attached to each factor. The information system's decision-making authority assigns relative values for these weights, depending on their mission priorities, before AoA is used to identify the most optimal system architecture.

The Figure of Merit Model

Let A_1, A_2... A_N be the *N* candidate architectures identified for an information system security architecture. Now, a linear mathematical function will be defined taking into account the *security strength*, *ease of use*, *performance*, and *cost* factors. To define this type of mathematical function, it is first necessary to identify the components of the candidate architecture A_i in terms of its components and the security controls within these components.

e(Ai) = E(Ai) / Max{E(Ai), i=1,2... n}, for i=1, 2...
s(Ai) = S(Ai) /Max{S(Ai), i=1,2... n}
F(A_i) = W_1 s(A_i) = W_2 e(A_i) = W_3 p(A_i) =
= E(Ai) / Max{ E(Ai), i=1, ... n}, for

Then, the FoM of an architecture A_i as shown in Equation 1, is defined as:

Equation 1

$F(A_i) = W_1\, s(A_i) + W_2\, e(A_i) + W_3\, p(A_i) + W_4\, c(A_i)$, where

$s(A_i)$ is the *security* index of A_i

$e(A_i)$ is the *ease of use* index of A_i

$p(A_i)$ is the *performance* index of A_i

$c(A_i)$ is the *cost* index of A_i.

Additionally, W_i are the weights associated with each factor representing its relative importance with respect to the other factors, contributing to the overall FoM function. The definition of the functions $s(A_i)$, $e(A_i)$, $p(A_i)$ and $c(A_i)$ are defined in the subsequent sections.

Security Index

The *security index*, $s(A_i)$ used in function $F(A_i)$ defined by Equation 1, represents the strength of the security of the architecture. This is estimated as follows:

Let the number of components comprising the architecture A_i be n and let S_i be the security strength of the ith component of A_i. If multiple security controls are implemented for the same component serving the same purpose (*e.g.,* user name and password, a biometric, or a certificate for authentication), then the *security strength* of the component is taken as the sum of the strongest of the controls and a fraction of the sum of the strengths of the other controls so as not to exceed 1.0. That is, if s_1, s_2, s_3 are the security strengths assigned to the same feature of a component, then the combined strength s of that feature would be:

Equation 2

$s = \min\{\max(s_1, s_2, s_3) + 20\%[\ \sum s_i - \max(s_1, s_2, s_3)\ ], 1.0\}$.

Here, the fraction percentage can be replaced by another reasonable fraction if the situation demands.*

Then the overall *security strength* of the architecture is computed as the sum of the security strengths of the components as:

Equation 3

$S(A_i) = \sum S_i$, where the summation is over all components comprising A_i, i=1, 2… n.

Here, the relative values for the security strengths of individual security controls S_i can be assigned by subject matter experts (SME) or security architects who are experts in security control assessment. A SME may assign numerical values for different types of authentication, for instance:

- Password—0.10
- Digital Certificate—0.15
- Security Token—0.25
- Smart Card—0.30
- Biometric—fingerprint 0.25—retina scan 0.40. [2]

Here, as we shall soon see, the absolute values do not matter as long as the relative strengths are kept in mind while assigning values.

The candidate architecture security strength computation procedure is repeated for all the architectures being analyzed in the AoA to obtain $S(A_i)$ i=1, 2… N.

For the FoM function to be uniformly sensitive to each factor, namely, *security strength*, *ease of use*, *performance*, and *cost*, these factors must be normalized. This mandatory step is needed because the factors represent totally different physical aspects of the architecture and have a wide value range spectrum. By normalizing each factor, the FoM function will be equally sensitive to all the factors and helps to identify the most desirable architecture conforming to the prioritizing of the information system. This security strength factor normalization step corresponds to dividing each candidate architecture security strength by the maximum of the security strengths among them. The resulting term is defined as the *security index*. That is, each architecture *security index* is given by:

Equation 4

$s(A_i) = S(A_i)\ /\mathrm{Max}\{\ S(A_i)\ , i\text{=1, 2… } N\}$.

Ease of Use Index

The second factor $e(A_i)$ in FoM function is a measure the *ease of use* of the system as would be experienced by the end user. Since this is something related to the end user, it can be characterized by the various use cases to be performed by the user. A representative of the end user appropriately assigns numerical values to these factors. This can be done either by going through the details of the operational use case diagrams (and if needed, management use cases) of the candidate architecture or by a hands-on run of operational simulators or rapid prototypes depicting the operational flow of the use cases and assigning values on a scale of one to ten.

In this case, the overall *ease of use* measure is defined in:

Equation 5

$E(A_i) = \sum E_i / m$, where the summation is over i=1, 2… m representing the m use cases for which the architecture is being designed. This procedure is repeated for all the candidate architectures to get the *ease of use* terms $E(A_i)$ for all candidate architectures i= 1, 2… N.

As in the case of security strength, *ease of use* measure is also normalized by dividing by the maximum of the values to get the *ease of use* index values $e(A_i)$ for i= 1, 2… N for all candidate architectures. That is:

Equation 6

$e(A_i) = E(A_i) / \text{Max}\{ E(A_i), i=1, 2\ldots n\}$, for i=1, 2… N.

Alternatively, *Apdex* measure, as will be defined in the case of performance index computation later in this article, can also be used for computing the *ease of use* index. [3]

Performance Index

The third factor in the FoM function is a measure of the estimated operational performance of the candidate architectures. This can be characterized by the response times for the use cases of the information system as mentioned earlier. The use case response times can be estimated using analytical performance models, [4] which can easily be built using each candidate architecture use case diagram. Once the response times for the m use cases are available, the overall *performance measure* for candidate architecture can be defined in two ways as outlined below:

- **Response Time:** Let $R_1, R_2\ldots R_m$ be the response times for the m use case in the case of the candidate architecture A_i. If the desired response times or response time thresholds $T_1, T_2\ldots T_m$ are specified as requirements, then the relative performance measure r_i for each use case is defined as:

Equation 7

$r_i = (R_i - T_i)/ T_i$ if $R_i > T_i$
$= 0$ if $R_i < T_i$.

In this case, the overall response time penalty for the candidate architecture is defined as:

Equation 8

$R(A_i) = \sum r_i$.

If the thresholds are not specified as part of the requirements, the total response time for the candidate architecture is defined as:

Equation 9

$R(A_i) = \sum R_i$.

In either case, the normalized *performance index* computed for each candidate architecture is:

Equation 10

$p(A_i) = R(A_i) / \text{Max}\{ R(A_i), i=1, 2\ldots N\}$,
for each candidate architecture i=1, 2… N.

- **Apdex Measure:** *Apdex* [5] is a numerical measure originally defined for measuring user satisfaction that provides a uniform way to report on the user experience. It assigns an Institute of Electrical and Electronics Engineers/Strategic Technology Office (IEEE/STO) single number on a scale of zero to 1 from a set of several measurements with zero for no user satisfied and 1 for all users satisfied. We propose using that concept for use case response time measurements in the following way:

As before, let $R_1, R_2\ldots R_m$ be the response times for the m use case in the case of the candidate architecture A_i, and let the corresponding thresholds be $T_1, T_2\ldots T_m$.

Define tolerances t_i as:

Equation 11

$t_i = 4.0 \cdot T_i$ for i =1, 2… m.

In this case, the *performance index* for the candidate architecture A_i is defined as:

Equation 12

$p(A_i)$= (number of use cases within their threshold) + 0.5 · (number of use cases within tolerance)/m.

By definition, this *performance index* already being the interval [0, 1] is automatically normalized when the computation of the performance index occurs. Note that *Apdex* can be computed only if the use case response time threshold is available.

Cost Index

The fourth factor in the FoM function F, defined in Equation 1, represents the candidate architecture *cost*, including the cost to own, operate, and maintain the various components. The cost of the overall system is computed as the sum of the costs C_i of the components of the candidate architecture. Therefore, the overall *cost* is:

Equation 13

$C(A_i) = \sum C_j$, where the summation is taken over all the components $j = 1, 2\ldots n$.

The component costs C_i can be further split into multiple factors, such as product and installation costs, training costs, and maintenance cost. This could help in providing more granularity in terms of priorities. For example, a particular information system might be able to allow higher product and training costs but not recurring costs such as maintenance and personnel costs when choosing architecture options. Such a differentially weighted cost factor is defined as:

Equation 14

$C_j = (W_{c1}C_1 + W_{c2}\,C_2 + W_{c3}\,C_3)\,/(W_{c1} + W_{c2} + W_{c3})$, for $j = 1, 2\ldots n$.

Here C_1, C_2, and C_3 are the product, training, and life cycle costs respectively of the *j*th component of architecture. W_{ci} are the relative weights for the three types of costs defined for each component (subscript *j* is omitted here to avoid clumsiness in the expression). The division by sum of the weights is to make sure total weighting of all the factors is 1.

As before, once the candidate architecture's overall cost is computed, costs are normalized by dividing by their

1	2	3	4	5	6	7	8	9	10
Option	**Distributed/ Centralized**	**Certification Validation**	**Caching?**	**Qualitative Remarks**	**Security Index**	**Ease of Use Index**	**Performance Index**	**Cost Index**	**FoM**
1	All Services Distributed	CRL* for certificate validation	Caching	Fast Slow Fast, Low High Low Secure, High Low Low Cost, High High Low Usability	0.79	0.91	0.89	0.80	1.79
2	All Services Distributed	CRL for certificate validation	No Caching	Fast Slow Slow, Low High High Secure, High Low High Cost, High High High Usability	0.88	1.00	0.76	0.89	1.76
3	All Services Distributed	OCSP** for certificate validation	Caching	Fast Fast Fast, Low Low Low Secure, High High Low Cost, High Low Low Usability	0.66	0.77	1.00	0.70	1.73
4	All Services Distributed	OCSP for Certificate Validation	No Caching	Fast Fast Slow, Low Low High Secure, High High High Cost, High Low High Usability	0.78	0.89	0.87	1.00	1.54
5	All Services Centralized	CRL for Certificate Validation	Caching	Slow Slow Fast, High High Low Secure, Low Low Low Cost, Low High Low Usability	0.87	0.79	0.76	0.91	1.51
6	All Services Centralized	CRL for Certificate Validation	No Caching	Slow Slow Slow, High High High Secure, Low Low High Cost, Low High High Usability	1.00	0.91	0.68	0.78	1.81
7	All Services Centralized	OCSP for Certificate Validation	Caching	Slow Fast Fast, High Low Low Secure, Low High Low Cost, Low Low Low Usability	0.76	0.66	0.89	0.80	1.51
8	All Services Centralized	OCSP for Certificate Validation	No Caching	Slow Fast Slow, High Low High Secure, Low High High Cost, Low Low High Usability	0.86	0.79	0.78	0.89	1.54

* Certificate Revocation List (CRL)

** Online Certificate Status Protocol

Table 1 Architecture options

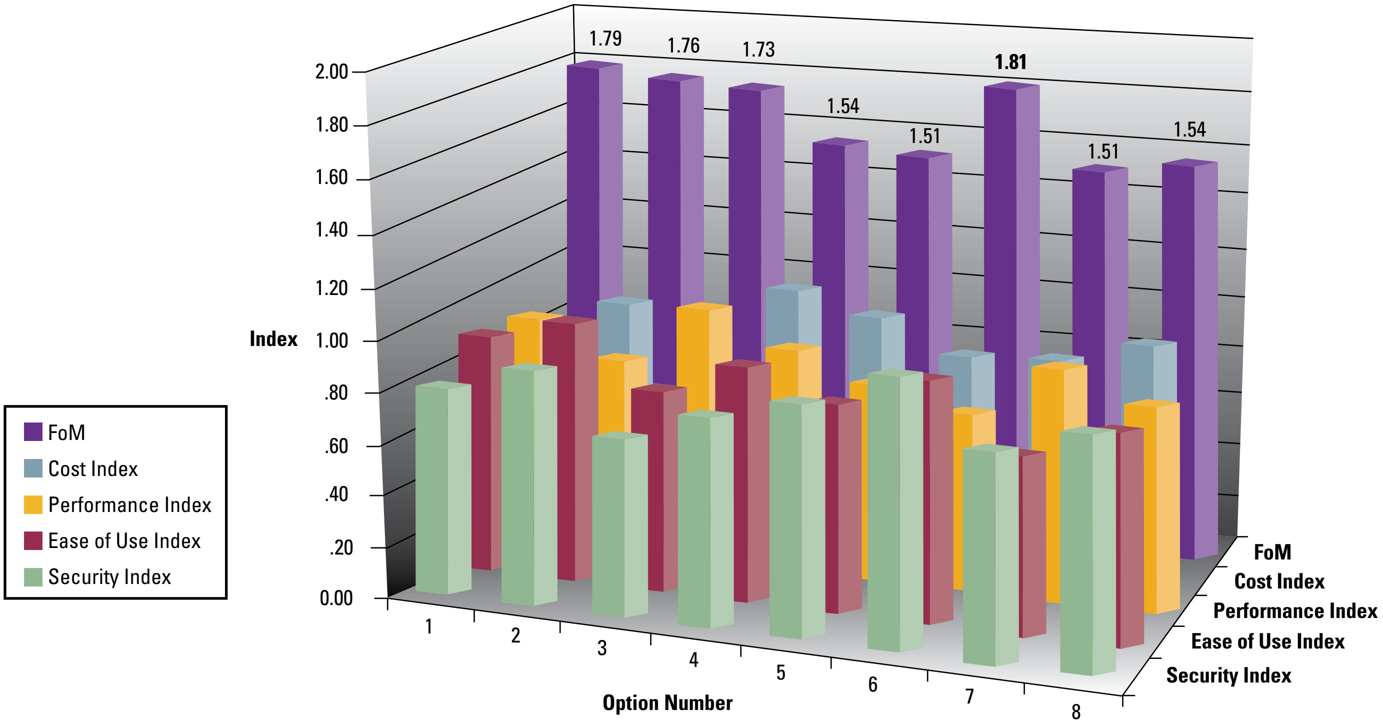


Figure 1 FoM and its factors for various options

maximum value, resulting in a *cost index* for each architecture option:

Equation 15

$c(A_i) = C(A_i) / \mathrm{Max}\{ C(A_i), i=1, 2... N\}$, for each candidate architecture $i=1, 2... N$.

FoM Computation

Once each candidate architecture *security* index, *ease of use* index, *performance* index, and the *cost* index are computed, the FoM function is calculated using this equation if Equation 10 is used for computing the *performance* index:

Equation 16

$$F(A_i) = W_1\, s(A_i) + W_2\, e(A_i) - W_3\, p(A_i) - W_4\, c(A_i)$$

If Equation 12 is used for computing the *performance* index, then Equation 17 is used to calculate FoM:

Equation 17

$$F(A_i) = W_1\, s(A_i) + W_2\, e(A_i) + W_3\, p(A_i) - W_4\, c(A_i)$$

Note that subtraction of the third and fourth terms in Equation 16, and the fourth term in Equation 17 occurs because (unlike *security*, *ease of use*, and *Apdex*) these terms are not the merits of the architecture, but are in fact demerits. Therefore, candidate architectures that provide the least value for these are preferred to gain a higher value of FoM.

Application to an Example

To demonstrate the practical application of the FoM concept, assume that we are performing an AoA of an architecture for a hypothetical assured information sharing system with typical use cases, such as user login, document discovery, retrieve, and create operations on the document server. Consider a simple architectural decision problem for this system.

Table 1 shows the various options we chose, such as: whether the services (identity authentication service, policy decision/enforcement, attribute store, document store, server, *etc.*) are distributed or centralized; whether Certificate Revocation List (CRL) or Online Certificate Status Protocol (OCSP) is used for certificate validation; or whether or not the identity assertions, attributes, and other data, if any, are cached. These are depicted in columns 2 through 4 in Table 1. Entries in column 5 indicate the qualitative remarks for each option in terms of FoM factors. For example, the term FastSlowFast in the first row of column 5 indicates that the response times for option 1 is fast because services are distributed, slow because the certificate validation scheme is CRL, and fast because caching occurs. Now, the value for the factor *performance* will be derived based on all these three contributing factors. This is also repeated for the other factors (*e.g., ease of use*, *security*, and *cost*). The values are then assigned in columns 6 through 9 and are based on the qualitative remarks in column 5 for each option. The architecture option's *security strength*, *ease of use*, *performance*, and *cost* values are then normalized (as described before) and replace the original values in columns 6 through 9. Figure 1 depicts these normalized values along with their corresponding FoM values. This chart clearly shows that option 6 is the most

The FoM mathematical model can evaluate candidate information system security architectures to aid architectural decision-making. This article presents FoM's mathematical form and function and derives the various factors comprising it.

meritorious option when uniform weights are chosen across the factors, based on FoM values.

While we have used uniform weights for the various FoM factors in this simple example, in an actual case, non-uniform weights can help in assigning relative importance to factors as needed and in not over-or-under emphasizing the importance of any factor in the decision-making process.

Application Notes

As mentioned, the example presented above is an over-simplified one with values derived from engineering judgment; no attempt to get realistic values is made. In an actual AoA, analytical performance models can be used to compute the performance measures, and simulation or other models can be used for generating *ease-of-use* estimates, while *cost* can be estimated by actually plugging in the necessary data. Anyone interested may contact the author to get more information on how to compute the *performance index*.

Benefits of FoM Model

The FoM concept defined in this article to compare multiple candidate architectures has several inherent benefits:

- Helps repeat and justify architectural decision-making
- Facilitates what-if information system analysis for varying priorities or focus
- Facilitates component–wise analysis in making informed security investment decisions in a modular fashion
- Helps to assess relative merits of various commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) solutions even for a given architecture
- Helps to tune the configuration of a chosen architecture in a dynamically varying environment
- Helps compare overall merit between current architecture and proposed enhancements.

Conclusions

The FoM mathematical model can evaluate candidate information system security architectures to aid architectural decision-making. This article presents FoM's mathematical form and function, and derives the various factors comprising it. This article also demonstrates the concept by applying it to a hypothetical assured information system design decision-making problem. Some of the model's benefits are that it helps repeat and justify architectural decision-making and it helps project the overall architectural merit for dynamic environments with changing priorities. ■

** The fraction percentage in Equation 2 is a number based on judgment of how significantly the <u>security strength</u> is affected by the strengths of the various controls for a component. Determining a quantitative method for assigning this fraction percentage is one area of focus for future research.*

References

1. Belur, Sheela and Gloster, Jonathan, "Mathematical Model for Security Effectiveness Figure of Merit and Its Optimization," Presented at SPIE Defense & Security Conference, April 2008 - Proceedings of the SPIE, Volume 6973, 2008
2. Belur, Sheela and Gloster, Jonathan, "Development of a Model for Assessing Impact of Information Assurance Functionality on Secure Messaging System Performance," Presented at SPIE Defense & Security Conference, April 2007 - Proc. SPIE, Vol 6570, 2007
3. Authentication Strength, *http://www.authenticationworld.com/Authentication-Strength/*
4. Belur, Sheela, "Performance Comparison of Certificate Validation Approaches," Internal Technical Note, VDTG, Jan 2007.
5. Application Performance Index—Apdex Technical Specification, Version 1.1, Apdex Alliance, Jan 2007, *http://www.apdex.org/documents/ApdexTechnicalSpecificationV11_000.pdf*

About the Author

Dr. Sheela Belur | is currently a freelance consultant, and her areas of interest are modeling, simulation, performance analysis, and optimization. Earlier in Van Dyke Technology Group, Columbia, MD, she was involved in performance modeling of enterprise security management systems. She has several years of experience in both Aerospace and information technology fields supporting several NASA and FAA contracts while being employed in CSC and Hughes. She has published several technical papers in open literature and has also served as a reviewer for many journals and conferences. Dr.Belur received her Bachelor's, Master's, and Doctoral degrees in mathematics from Bangalore University, India.

Upstream Intelligence Use Cases

(Article 6 of 7)
by Tyson Macaulay

The Upstream Intelligence articles included in this edition are part of a seven article series. Readers can find all previous articles in the Summer and Fall 2010 editions of the IAnewsletter.

Upstream Intelligence (UI) and security is about leveraging the capabilities of telecommunications carrier infrastructure as a new layer of organizational security, complementing the traditional layers that start at the organizational, network perimeter. UI can be derived from at least five existing capabilities found in a typical carrier infrastructure: traffic flow analysis, domain name services (DNS), messaging filtering services, peer-to-peer management, and Web proxy services. (See articles 1 and 2 in this series—Summer 2010 *IAnewsletter* edition).

In this article, we discuss a few sample use cases for UI in the context of vulnerability and threat management. Some of these use cases center around a particular carrier infrastructure capability, while others reflect the more sophisticated requirement for correlation of data from multiple assets to increase the accuracy and assurance of the results.

Threat and Vulnerability Assessment

Threat and Vulnerability Assessments (TVA) are well understood processes of analyzing the threats aligned against an asset, whether it possesses addressable or intrinsic weak points, and what can be done about the situation. Ideally, a TVA may be performed by a third party or internal audit group. A TVA should be able to cite evidence related to threat levels and agents and probe targets of evaluation from either remote locations (the Internet) or from local connections (LAN segment), searching for holes in the configuration or missing patches that allow for some form of attack to be executed successfully. Typically there are two fundamental weaknesses in the TVA process.

First, assessments of threat levels and threat agents are frequently intuitive, professional guesses, or based on entirely qualitative (non-precise, non-measurable) evidence.

The second typical weakness of TVAs is that they are assessing only the means of success of an attack, if one were to occur. In other words, if someone attacks, what are the weak points through which they may experience success? The result is almost always speculative, which enables those who are so inclined to defer, diminish, or dismiss security recommendations for lack of hard evidence.

UI greatly improves the TVA process by: a) providing quantitative (measurable) evidence of threat levels and agents, and b) providing quantitative evidence associated with the force and velocity of threats against given vulnerabilities. In other words, UI allows for not only probabilistic views of threat, but measurable assessment of actual compromises and exposures.

Traffic Flow Exposure Assessment

Figure 1 shows an example of how an exposure assessment (EA) can be undertaken by the application of the UI capabilities of traffic flow analysis. Traffic analysis from the carrier infrastructure can provide tangible, quantitative evidence of exposures (manifest threats). First, command and control (C&C) traffic becomes visible through UI, and the observation of C&C traffic destined to an enterprise perimeter is potential evidence of compromised internal devices. More alarmingly, C&C traffic leaving an enterprise perimeter (probably obfuscated in Web traffic) is positive indication that a vulnerability not only exists but has been exploited successfully. "Darkspace" is IPv4 (or v6) address space which is allocated but not assigned, meaning that it can be routed to a network, but there is no machine with the assigned IP address to receive the traffic. Observing darkspace is very useful for measuring the levels of threat-against and compromise-profile of a given entity, because there is no legitimate reason for devices to be querying darkspace. [1] To the extent that an organization's darkspace is being "hit" by scans and other traffic, it is a quantitative threat indicator and metric. To the extent traffic from an organization is destined for darkspace, it is an indicator that internal, compromised devices are

probing for other targets to exploit from their location.

Beyond traffic flow analysis, other UI capabilities can be applied to TVAs to obtain quantitative threat and vulnerability metrics.

Message Filtering Exposure Assessment

While inbound spam messaging is ubiquitous, outbound spam from an organization is a strong indication of the presence of compromised devices (as we will discuss in the seventh article in this series).

Inbound spam is the virtual junk mail that is sent to all organizations with an Internet presence from a combination of disreputable Internet service providers (ISP), compromised devices which have been pressed into service as spam engines, and e-mail accounts which have been compromised. Between 95% and 98% of the e-mails received by Internet-facing messaging servers is illicit or infected: spam, phishing messages, and viruses. Increasingly, inbound message filtering is being outsourced to upstream service providers with dedicated infrastructure for this purpose. Messaging security outsourcing is becoming popular because it reduces the costs associated with bandwidth, software licenses, human capital, and machine capital.

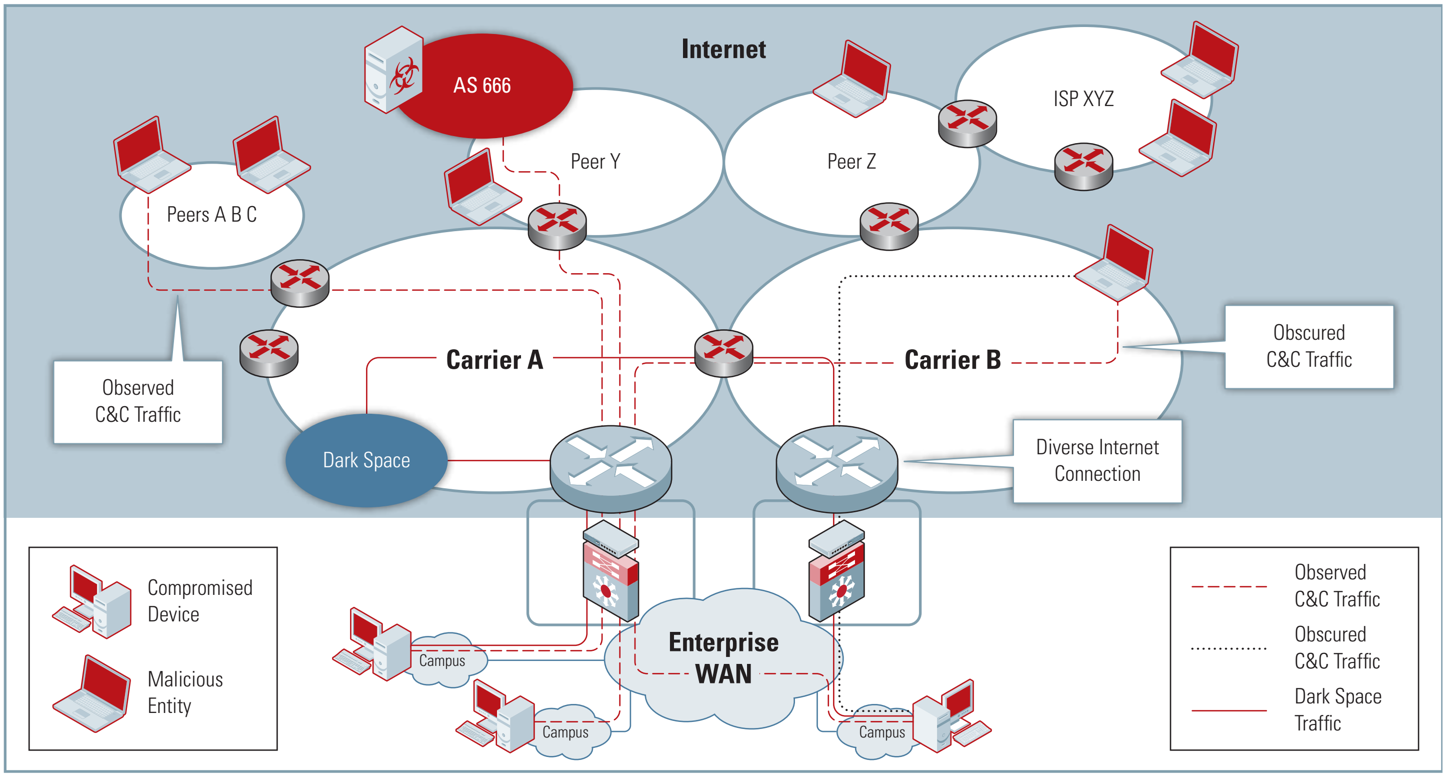


Figure 1 Enhanced Vulnerability Assessment with Upstream Intelligence

Illicit forms of messaging may also be exiting a given organization through the legitimate messaging servers and from legitimate user accounts. Devices which have been compromised by malware will frequently be put to work for this purpose. Through C&C channels, compromised devices will download pre-formatted spam messages and address lists for millions of external targets. Once these engines are activated, they can generate thousands of messages per hour from a single device. The impact on messaging infrastructure in these cases would be obvious. However, not all malware will apply a brute-force approach or noticeably abuse systems. Compromised devices may generate messages at a much lower volume so as not to degrade message infrastructure. Or, as was the case in the 2010 Ghostnet affair, compromised devices could be used for targeted "spear phishing" attacks, leveraging the good reputation of the host organization to penetrate other organizations. [2] In either case, outbound message filtering is critical to assessing the presence of compromised devices to obtain threat and vulnerability metrics for a measurement of exposure.

Domain Name Services Exposure Assessment (EA)

Like traffic flow and messaging, Domain Name Services (DNS) seeded with UI about malware C&C domains is another very important source of exposure assessment for any organization. In fact, DNS analysis, combined with messaging analysis, is probably one of the most effective forms of EA that can be done within the enterprise perimeter. For instance, DNS services within the enterprise or re-directed to specialized upstream DNS servers can be configured to alert whenever an internal device looks up a known C&C domain. Better yet, the DNS service can be configured to beneficially "poison" the DNS by returning a special internal IP address where attempts to create C&C flows are quarantined, and any traffic destined for exfiltration can be gathered for later analysis. The primary limitation associated with DNS EAs is that the list of bad domains can change incredibly fast—a practice known as "fast flux"—making the management of DNS grey lists a task often beyond the resources of individual organizations.

Peer-to-peer Exposure Analysis

For most organizations, the existence of any peer-to-peer (P2P) traffic is usually a bad sign, because so much P2P software is malware in disguise. A P2P exposure analysis is about detection and alerting on the presence of P2P traffic coming out of the corporate network or within the corporate network. This can be accomplished within the corporate wireless area network (WAN) environment if the tools exist, or it can be accomplished upstream. Given that P2P management infrastructure is typically already deployed by carriers upstream, it is often more cost-effective to leverage an existing infrastructure rather than deploy a P2P management infrastructure internally for exposure analysis support.

Cloud Computing

For a formal description of cloud computing and the business models available, please refer to sources such as the National Institute of Standards and Technology (NIST). [3] Unfortunately, the length of this article does not allow us to engage in a discussion related to the overall security pros and cons of cloud computing. The following cloud computing discussion is truly minimalist, intended merely to support a discussion of the benefits of UI in the context of cloud computing.

Computing in the cloud may be a private or a public affair. Private clouds may involve total ownership of the infrastructure, including the physical site, or a dedicated infrastructure managed by a supplier. A public cloud platform is generally accessible to the open Internet and anyone who wants to subscribe to (buy) a piece of the cloud. Hybrids of public/private might be a shared infrastructure but dedicated platform instances or possibly private network links.

A substantial percentage of cloud computing deployments will be "public" or "hybrid" in nature, meaning that they share some or all of the infrastructure with other organizations. Salesforce.com is a good example of a "public" software-as-a-service (SaaS) cloud. Alternative cloud models are frequently described as platform-as-a-serve (PaaS) and infrastructure-as-a-service (IaaS). Figure 2 outlines how these cloud computing models differ from a functional and a security perspective. The high level message contained in Figure 2 is that the more versatile the cloud solution the more security responsibilities are assumed by the client organization. [4]

Security Benefits of Cloud Computing

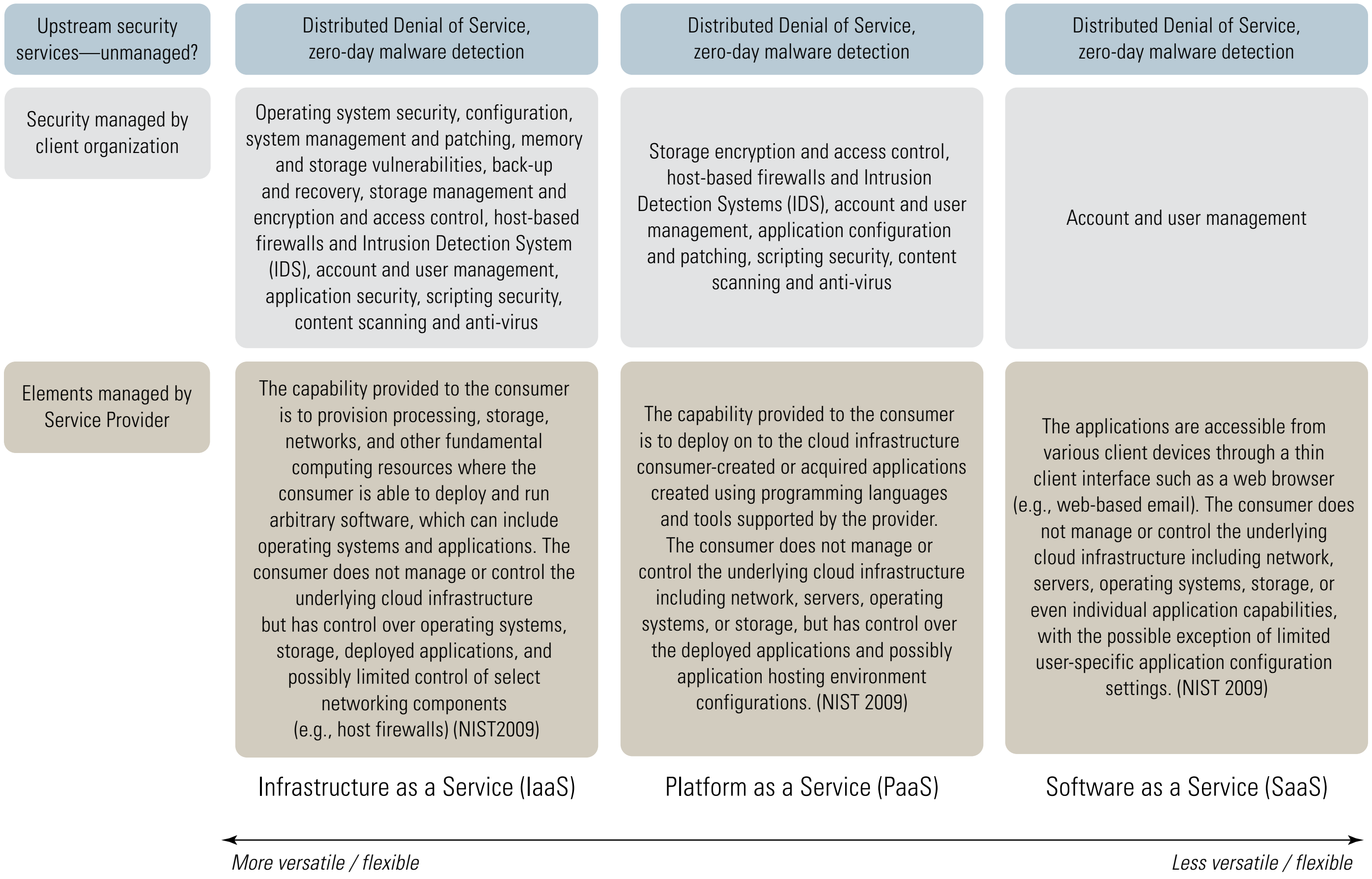
Cloud computing can offer substantial security benefits to organizations. A significant amount of infrastructure, operating system/platform, and application security can be outsourced, and liability, but not necessarily risk, can be contractually transferred to reduce costs.

While the applications and platforms deployed within a cloud will probably possess some of the same vulnerabilities of stand-alone infrastructures, they can have the benefit of a dedicated security team supporting several clients and efficiently spreading costs over a much larger infrastructure. Most noticeably, clouds can be more resilient against the potent threat of distributed denial-of-service (DDoS). For instance, cloud-based systems are often highly diverse (many geographically unique network access points) and balanced (demand can be shared among physically unique data centers). This can make the assets within these clouds more stable under variable demand or attack.

Cloud Security Challenges

Subscriber DDoS

If the Internet is the basis of organizational access to the cloud services, then DDoS attacks can essentially cut off access to critical, cloud-based corporate assets such as e-mail, customer relationship management or enterprise resource planning (CRM/ERP) applications, or client service Web sites and store-fronts which are based in the cloud. While the cloud-based services remain available on the



	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Upstream security services—unmanaged?	Distributed Denial of Service, zero-day malware detection	Distributed Denial of Service, zero-day malware detection	Distributed Denial of Service, zero-day malware detection
Security managed by client organization	Operating system security, configuration, system management and patching, memory and storage vulnerabilities, back-up and recovery, storage management and encryption and access control, host-based firewalls and Intrusion Detection System (IDS), account and user management, application security, scripting security, content scanning and anti-virus	Storage encryption and access control, host-based firewalls and Intrusion Detection Systems (IDS), account and user management, application configuration and patching, scripting security, content scanning and anti-virus	Account and user management
Elements managed by Service Provider	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls) (NIST2009)	The capability provided to the consumer is to deploy on to the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. (NIST 2009)	The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. (NIST 2009)

Figure 2 Cloud computing security stack

Internet, they become unavailable to subscribing organizations as illustrated in Figure 3.

Abbreviated Visibility

The type of cloud service purchased (SaaS, PaaS, IaaS) may mean giving up visibility of multiple security layers because the shared nature of the infrastructure means that security issues with other clients would be become visible if access is granted. For instance, intrusion detection alerts are kept strictly internal to the service provider. Even if some visibility is afforded, it is still possible that influence over configuration, alerting levels, and alarm management will be unavailable, since these security controls may be shared across many clients and cannot be turned off or on for any given client.

Monocultures and Proprietary Technology

Clouds may possess security issues associated with monocultures or opaque, proprietary technology. A monoculture exists when the identical operating system or application configuration is used throughout the cloud. While this makes administration effective and keeps clouds super efficient, it also means that a single unique vulnerability can impact across clients. Some clouds use proprietary infrastructure platforms or even highly customized operating systems. This infrastructure is an essential part of their competitive advantage and details are not publicly available, let alone published for third-party scrutiny. "Security through obscurity" is a practice not considered optimal, because vulnerabilities tend not to be researched and dealt with in the same manner as with more open systems. In proprietary systems, exploits may go undetected longer if only a small community of administrators are tasked with reviewing and assessing security, trying to understand what abnormal operations and traffic look like in the first place.

Closing the Cloud Computing Security Gaps

Upstream security and intelligence can close the DDoS vulnerability by providing security controls in the carrier network, ensuring that enterprises do not lose access or control over cloud-based resources. Even multi-homing (two or more egress points from the corporate network to the Internet) will provide little assurance against a DDoS attack. The alternative to DDoS protection are dedicated, private links to the cloud service, unfortunately a feature which is a system of not available from all cloud providers.

Upstream intelligence can address the cloud gaps of abbreviated visibility,

Cloud DDoS Victim

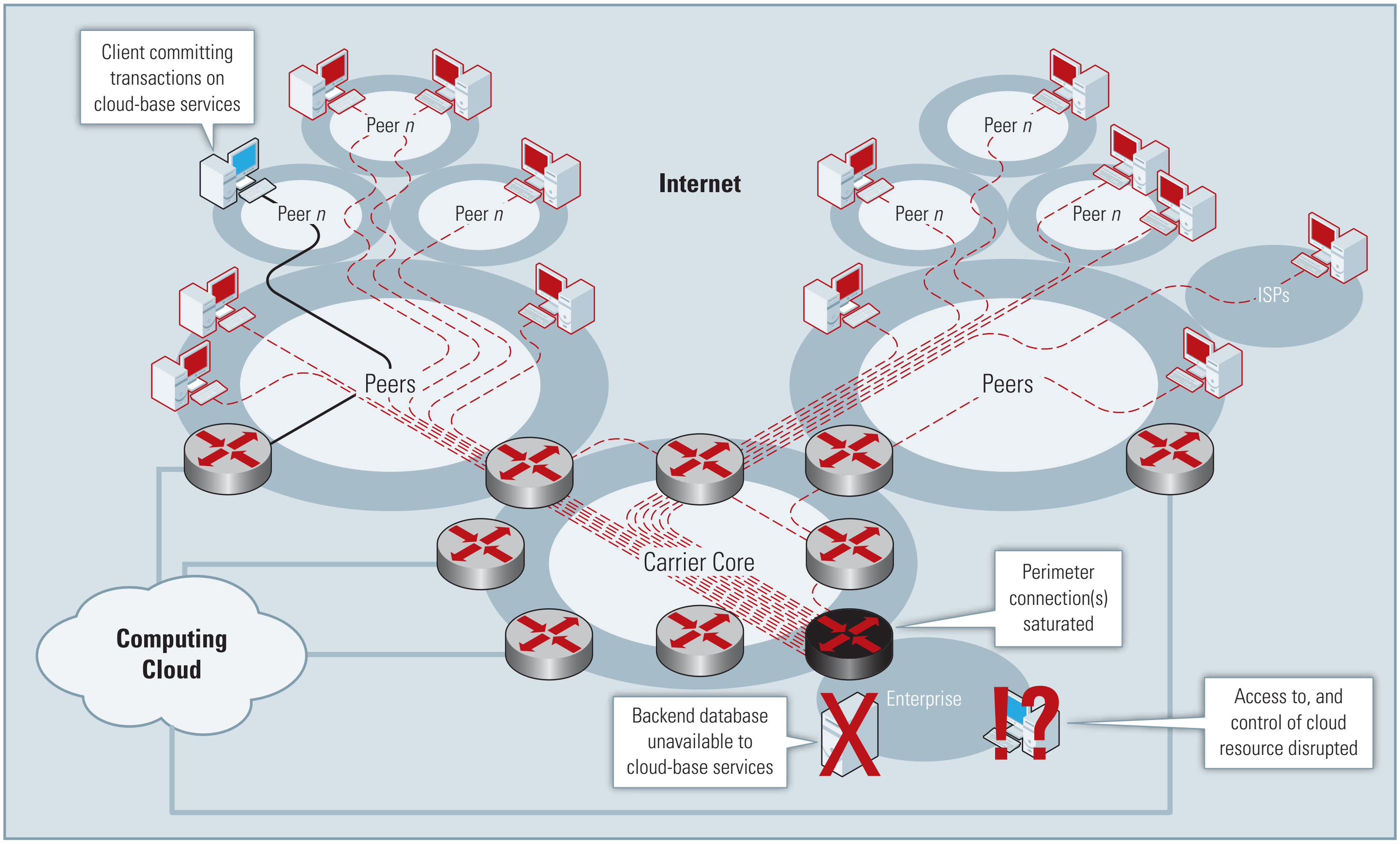

Client committing transactions on cloud-base services
Peer n
Peer n
Peer n
Internet
Peer n
Peer n
Peer n
ISPs
Peers
Peers
Carrier Core
Computing Cloud
Perimeter connection(s) saturated
Enterprise
Backend database unavailable to cloud-base services
Access to, and control of cloud resource disrupted

Figure 3 Cloud DDoS victim

monocultures, and proprietary technology by virtue of the fact at any cloud service provider will be logging and reporting usage statistics to subscribers. The ability to review and compare logs against upstream grey lists and establish alerting rules—if not access policies (depending on the service provider and application/service type)—empowers the cloud subscriber to add an additional, highly effective and proactive layer of security with little to no impact on the service or the service provider.

Conclusion

Threat and vulnerability assessment has become a bread-and-butter operational practice for many organizations, but it can be substantially improved through the UI metrics related to threat, exposure, and compromise rates.

Cloud computing services are incredibly powerful and beneficial. The Internet is clearly moving towards widespread adoption of such services, for both large and small entities. But the new operational framework and efficiencies that cloud-services represent can also come with a number of security dependencies and risks; some of these risks can only be addressed through upstream security and intelligence capabilities. ■

References

1. See "Anatomy of Upstream Security," IAnewsletter Volume 13, no. 3, for a discussion of "threat-to" versus "threat-from" - *http://iac.dtic.mil/iatac/download/Vol13_No3.pdf*
2. See *http://en.wikipedia.org/wiki/Infowar_Monitor* and *http://www.mcafee.com/us/threat_center/operation_aurora.html* and *http://www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0*
3. See *http://csrc.nist.gov/groups/SNS/cloud-computing/index.html*
4. Cloud Security Alliance Guidelines 2.0, see *http://www.cloudsecurityalliance.org*

About the Author

Tyson Macaulay, CISSP, CISA | is a security liaison officer for Bell Canada with 18 years of Information and Communication Technologies (ICT) security experience. Mr. Macaulay works on security and risk management solutions for the largest organizations in Canada. He also supports the development of engineering and security standards through organizations like the International Organization for Standardization (ISO), and is a university lecturer and author of three books and many published papers. His books include: Securing Converged IP Networks (2006), Critical Infrastructure: Threats, Risks and Interdependencies (2008), and Industrial Control System Security (forthcoming 2010). Mr. Macaulay's work on upstream intelligence has been driven by the need to proactively address the increasing frequency, longevity, and severity of undetected ICT compromises, which are threatening international security and prosperity. Further research and references are available at *http://www.tysonmacaulay.com.*

Ask the Expert

by Chris Silva

Increasingly, however, the debate around cloud is shifting away from the IT implications of these solutions and instead focusing on the risk profile associated with these partners, as it should.

Cloud computing has been a major topic of interest across information technology (IT) departments. In information security circles, the debate on whether or not to enter into the cloud has reached a tipping point as the supporters, and adopters of the technology now outweigh its detractors, and yet in many organizations an overall lack of understanding about what risk factors surround the cloud exist. The cloud has been a topic of so much interest that the *IAnewsletter*, Spring 2010, was dedicated to the topic, including a cover story. In the article, written by Brett Michael and George Dinolt, the authors responded to a previous "Ask the Expert" column by expanding on details unique to each of the models for cloud computing and outlining the various definitions of cloud. Models for engagement with a provider were also discussed through infrastructure and data security scenarios in light of a move to cloud. Increasingly however, the debate around cloud is shifting away from a pure focus on the IT implications of these solutions and expanding to focus on the risk profile associated with these partners, as it should. In most cases, the protections for handling, storing, securing, and providing access to data within a cloud partner's facility will equal or trump those protections in place within most organizations. The issue of risk, if we take the definition from the Cloud Security Alliance, centers on seven areas of specific threat. [1] These areas bring forth a common theme, one we often cite to clients: mastering third-party partner management, sourcing, and service level agreement (SLA) development. Mastering these core elements of sourcing and vendor management can mean a more secure cloud experience, no matter what the model of cloud being considered.

Below are some best practices for managing relationships to mitigate third-party risk when considering the cloud. These areas should be at the heart of any risk profile or partner analysis for taking on a partner for any cloud computing model:

- **Infrastructure:** Will the infrastructure be dedicated or shared? Will data physically reside in a specific data center or is the infrastructure virtualized?
- **Availability:** What is the availability and what are the risks? Does the service provider have backup power generation? Air-conditioning? Is the provider exposed to floods or earthquakes? What are their backup plans?
- **Controls:** What controls does the provider have in place? What is their change control process? What are their testing processes? How frequently do they test?
- **Regulation:** Does the provider fall under regulatory oversight and have experience complying with regulation?
- **Reputation:** Is the provider a large, reputable company that has invested in infrastructure, availability, controls, and brand? Are they an industry leader? Does the service provider have much to lose from a breach and therefore have a motivation to work hard to prevent one? Or are they a small company that will say anything to get a sale?
- **People:** Who are the provider's employees? What are their backgrounds? What background checks have been conducted? What training processes are in place? Is there a separation of duties?

It's important to note that each bullet above should act merely as a catalyst for

▷▷ continued on page 33

IATAC SPOTLIGHT ON A UNIVERSITY

National Defense University

by Angela Orebaugh

The National Defense University (NDU) is a national level senior service college and the premier center for Joint Professional Military Education (JPME). NDU is under the direction of the Chairman, Joint Chiefs of Staff and its mission is to "prepare military and civilian leaders from the United States and other countries to evaluate national and international security challenges through multi-disciplinary education and research programs, professional exchanges, and outreach". [1] NDU is an internationally recognized graduate-level university with five colleges and multiple centers of excellence focused on education, research, and outreach in national security matters. With campuses in Washington, D.C., and Norfolk, VA, the University's reach and influence extends to U.S. and international constituents with students from more than 60 countries worldwide attending annually. [2] NDU's five colleges are:

- College of International Security Affairs (CISA)
- Industrial College of the Armed Forces (ICAF)
- Information Resources Management College (*i*College)
- Joint Forces Staff College (JFSC)
- National War College (NWC).

NDU also offers an Information Operations Concentration Program (IOCP), which complements ICAF's core curriculum. IOCP includes courses on information assurance and strategy.

NDU *i*College prepares leaders to direct the information component of national power by leveraging information and information technology for strategic advantage. Primary areas of expertise include: leadership; process management; information technology, policy, and security; transformation; and management of acquisition processes and reform. [3] NDU *i*College offers seven programs of study including Information Assurance (IA). The IA program has been recognized by the National Security Agency (NSA) and the Department of Homeland Security (DHS) as a National Center of Academic Excellence (CAE) in Information Assurance Education (IAE) and offers the following certificates:

- NSTISSI No. 4011 certificate
- CNSSI 4012, 4016: NSTISSI 4015 certificate
- Chief Information Security Officer certificate (CISO)

The certificates prepare students to:

- Exercise strategic leadership in the development and use of information security strategies, plans, policies, enabling technologies, and procedures;
- Develop and lead programs to provide information security controls, security awareness training, risk analysis, certification and accreditation, security incident management, continuity of operations, and disaster recovery;
- Link people, processes, information, and technology to critical IA decisions; and
- Develop and lead, in accordance with laws and regulations, an enterprise IA program that promotes and attains national security, agency, and inter-agency goals. [4]

Students may apply their certificates, equivalent to at least nine graduate-level credit hours, toward selected Master's or doctoral degree programs at several partner institutions of higher education. Certificates include a diverse set of courses focusing on topics such as critical infrastructure protection, risk management, networking and telecommunications, cyber security, certification and accreditation, continuity of operations, and cyberlaw. ■

References

1. *http://www.ndu.edu/info/about_ndu.cfm* and *http://www.ndu.edu/info/mission.cfm*
2. *http://www.ndu.edu/info/NDU%20Factsheet.pdf*
3. *http://www.ndu.edu//iCollege/index.html*
4. *http://www.ndu.edu//iCollege/pcs/pcs_ia.html*

Dr. Daniel Kuehl

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 SME profiled in this article is Dr. Daniel Kuehl at National Defense University (NDU).

Dr. Kuehl is a professor in the Information Operations and Assurance Department at NDU *i*College. He spent 22 years on active duty in the United States Air Force before joining *i*College (formerly and formally known as the Information Resources Management College or IRMC) in 1994. In his military career, his assignments included serving as a staff officer at the Pentagon and working as a nuclear planner for HQ Strategic Air Command at Offutt Air Force Base. Since joining the *i*College faculty, Dr. Kuehl has delivered lectures to a wide range of Department of Defense (DoD), Allied, and international institutions, as well as maintained his memberships and networks in a number of key professional associations.

Dr. Kuehl's areas of scholarly interest include military and national security strategy, information warfare/operations, military and diplomatic history, operational planning, public diplomacy/strategic communication, and critical infrastructure protection. He has published and presented widely on these subjects and has served on a number of dissertation committees. [1]

Dr. Kuehl received his BA from Allegheny College, his MA from Temple University, and his PhD from Duke University, all in history. He teaches a number of NDU *i*College courses that are available to students attending the National War College or the Industrial College of the Armed Forces (ICAF), as well as students enrolled in one of the *i*College's several certificate programs. These courses include "Information Engagement and Strategic Communication" (SCL); "Information Power and National Security" (IOS); and "Information Operations in Theater Strategy" (IWS). ■

References

1. *http://www.ndu.edu/iCollege/facultystaff/kuehl.htm*

IA Connect

Trying to research information about a particular information assurance (IA) vendor or product? Or want to know who within the Department of Defense (DoD) has used a particular IA product and what their experience was? IA Connect is the one-stop shop to bring you the most up-to-date information on IA products, solutions, and services. It provides a forum to share knowledge and experiences of IA products, solutions, and services within the DoD community. By visiting the IA Connect Knowledge Center Beta, you can participate in our pilot program and help keep the DoD community well informed of current IA technologies. In the Knowledge Center, you can view historical use of products within the DoD, including product implementation and user experiences. You can learn if others within the Department share your interest in a product or vendor. You can also view a record of DoD meetings with vendors. To access the IA Connect Knowledge Center, visit *https://nii.iaportal.navy.mil/login.htm*. You will need a Common Access Card (CAC) and *.mil* e-mail address to access the site.

Increase Your Awareness with Collaboration

by Cheryl Bratten

Separately, DoDTechipedia and Aristotle offer useful data, but when used together they provide a powerful knowledge base presenting situational awareness of the DoD S&T enterprise.

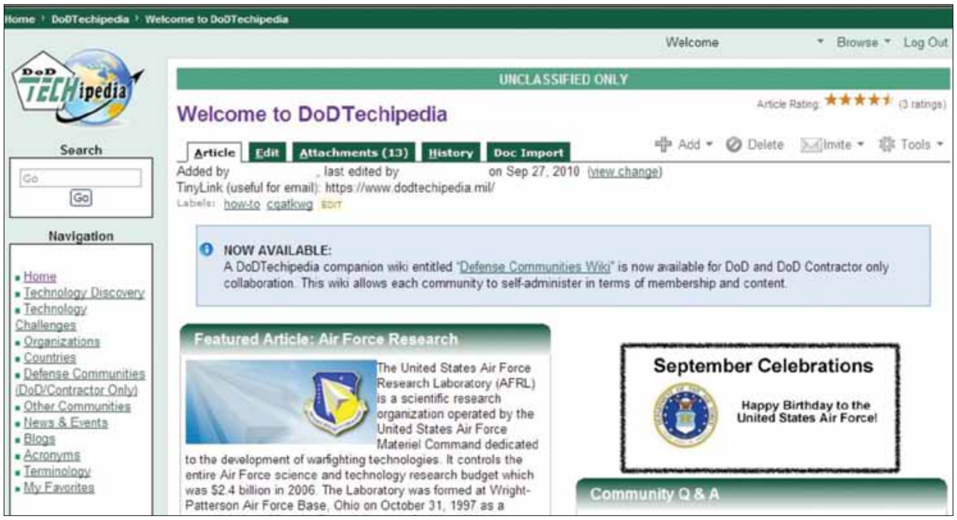
Are you looking for solutions to securing critical information in a cloud computing environment? Do you have expertise in defending the Global Information Grid (GIG)? Is your group developing policy for operations security with use of social media tools? Are you new to the Information Assurance (IA) community and need to get up to speed on what is happening across the Department of Defense (DoD) and federal government?

By collaborating with other IA professionals, you can increase the value of your limited resources by learning from the successes and failures of others, reducing the duplication of efforts, sharing your expertise, and reaching out to an extensive network of DoD and federal government professionals in your field. The Defense Technical Information Center (DTIC) has two tools that can increase your awareness through collaboration.

DoDTechipedia

Does your group need a secure space to collaborate? *DoDTechipedia*, which has been covered extensively in the *IAnewsletter*, is DoD's science and technology (S&T) wiki (Figure 1). Through DoDTechipedia you can post a question to the community in "Technology Challenges," research your topic through the search feature, and share your expertise by creating, populating, or editing a page. By creating a blog, you can update the community on the progress of your research projects and solicit the community's feedback. You can request a community space through the newly-released "Defense Communities Wiki" feature. As DoD civilians and DoD contractors, you can request a private space on DoDTechipedia and assign your own administrator. By creating a space for your specific work group or project, all key stakeholders can easily access documents and project elements in one location. Your community space administrator determines who can join and sets their collaboration capability.

DoDTechipedia provides the flexibility and security you need to collaborate across the research and engineering (R&E) community. A classified version of DoDTechipedia is also available on the SIPRNET.



Welcome to DoDTechipedia

Added by , last edited by on Sep 27, 2010 (view change)
TinyLink (useful for email): https://www.dodtechipedia.mil/
Labels: how-to cgatkwg EDIT

NOW AVAILABLE:
A DoDTechipedia companion wiki entitled "Defense Communities Wiki" is now available for DoD and DoD Contractor only collaboration. This wiki allows each community to self-administer in terms of membership and content.

The United States Air Force Research Laboratory (AFRL) is a scientific research organization operated by the United States Air Force Materiel Command dedicated to the development of warfighting technologies. It controls the entire Air Force science and technology research budget which was $2.4 billion in 2006. The Laboratory was formed at Wright-Patterson Air Force Base, Ohio on October 31, 1997 as a

September Celebrations
Happy Birthday to the United States Air Force!

Figure 1 DoDTechipedia offers users secure spaces to collaborate.

Aristotle

Launched in August 2010, *Aristotle* is DTIC's newest collaborative tool. Aristotle is a Web-based professional networking tool designed for federal government and DoD employees and contractors in the R&E community (Figure 2). Aristotle connects federal and DoD customers, users, and collaborators. It also provides a constantly evolving snapshot of what is going on across the R&E community. In addition, users can assign distribution codes and permissions to everything they create in or upload to Aristotle.

Aristotle helps make your search more efficient by returning results for people, projects, topics, and documents with one query. For example, if you enter "Global Information Grid" into the search box, it will return 1,917 people associated with the topic; 52,946 active and completed projects; and 22,088 topics associated with your search. If you click on a person from the search results, you will find the following information:

- Documents the individual is working on
- Published documents authored by the individual
- Groups he or she belongs to
- Professional associations
- Areas of expertise.

Select "graph view" to see a visual representation of how the selected person, project, or topic connects to the greater R&E community. You can subscribe to any person, project, or document and receive e-mail notification when it is updated.

Using DoDTechipedia and Aristotle in tandem increases the effectiveness of your work. By searching both tools before beginning your project, you can save time and resources by reviewing the successes and failures of other projects in your field. Separately, DoDTechipedia and Aristotle offer useful data, but when used together they provide a powerful knowledge base presenting situational awareness of the DoD S&T enterprise.

Access to both DoDTechipedia and Aristotle requires a free registration with DTIC. Registration with DTIC is open to all DoD and federal government employees and contractors. To register, visit *http://www.dtic.mil/dtic/registration.* Potential contractors and some academic institutions may apply for access through the Potential Contractors Program by following the instructions outlined on DTIC's Web site *(http://www.dtic.mil).*

DTIC is the premier provider of scientific, technical, research, and engineering information for the defense community. It has served the information needs of the defense community for 65 years. ■

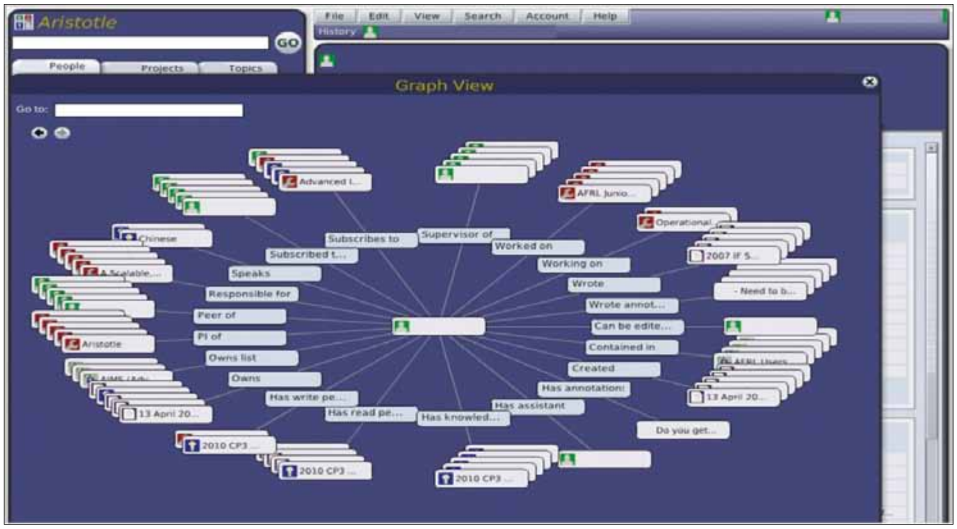


Figure 2 Aristotle's Graph View function allows users to see who and what a person is connected to

DTIC Information Resources:

DoDTechipedia, DoD's science and technology wiki:
https://www.dodtechipedia.mil

Aristotle, Professional networking for the DoD: *https://www.dtic.mil/aristotle*

DTIC Online (public site):
http://www.dtic.mil

DTIC Registration:
http://www.dtic.mil/dtic/registration

Survivability in Cyberspace Workshop: Learning How to Fight Through

by Dr. Kevin Kwiat and Patrick Hurley

In General T. Michael Moseley's Chief of Staff of the United States Air Force (CSAF) white paper, "The Nation's Guardians: America's 21st Century Air Force," he states that the Air Force's mission is to "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." The Survivability in Cyberspace Workshop purported to augment General Moseley's last goal by adding another capability within the cyberspace domain: to *fly* and *fight* and *fight-through*.

Here, *fight-through* carries the connotation of mission continuance even when damage is inflicted on Air Force cyber assets, so the notion of fight-through stands on the ability to sustain damage yet survive with mission assurance—a property referred to as survivability. Sustained survivability calls for recovering with immunity so as to be insusceptible to similar attacks. Leaders in the field of cyberspace survivability gathered at the Survivability in Cyberspace Workshop, a new international Air Force Research Laboratory (AFRL) event, to share and form approaches, both near and far term, to achieve a common goal—fight through attacks.

Unlike air or space, cyberspace differs in a fundamental way: air and space are natural settings, but cyber is man-made. As a made-made entity, cyberspace is composed of networking and information resources, so it is subject to human control and, therefore, human malice.

Failures caused by cyber attacks can have profound physical impacts. This is underscored by cyber physical systems (CPS). A CPS integrates computation, communication, and storage capabilities with the monitoring or control of the physical systems. Because a CPS can produce a pronounced and immediate physical impact, it must be operated safely, dependably, securely, efficiently, and in real time. By inextricably binding cyber assets to their environments, securing a CPS encompasses information and physical security; yet, the CPS's dual informational and physical nature increases its perimeter of penetration. This exposure to attack lends credence to seeking survivability for CPS.

The workshop's graphic (Figure 1) illustrates what is being sought: the ability to venture into cyberspace, endure damage, and achieve the goal of *fly* and *fight* and *fight-through*. Helping to address this pressing challenge, the workshop's co-chairmen and authors of this article, Dr. Kevin Kwiat and Mr. Patrick Hurley of the AFRL's Information Directorate, were granted financial support from the Air Force European Office of Aerospace Research and Development (EOARD), and their inaugural event became part of CPSWEEK 2010—the world's leading symposium on CPS—held in Stockholm, Sweden.

Among the major talent attracted to the AFRL event was Dr. Per Martin-Löf, Swedish logician, philosopher, and mathematical statistician, who is internationally renowned for his work on the foundations of probability, statistics, mathematical logic, and computer science. Focused primarily on the research ahead, the workshop's participants engaged in the emerging topic of CPS, by aiming their attention at the interactions between the physical-world and computational-world processes. Their view, however, was taken through the prism of survivability. ■

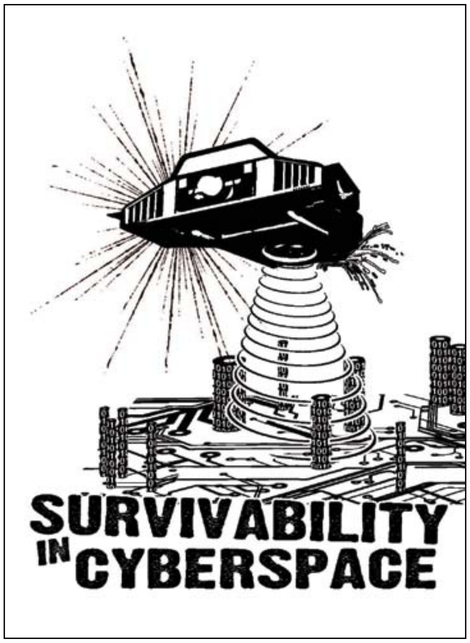


Figure 1 This Survivability in Cyberspace Workshop graphic depicts the Air Force's cyber goals: fly, fight, and fight-through.

About the Authors

Kevin Kwiat | is a computer engineer with the U.S. Air Force Research Laboratory's Information Directorate in Rome, NY, where he has worked for more than 27 years. He received a BS in computer science and a BA in mathematics from Utica College of Syracuse University, and a MS in computer engineering and a PhD in computer engineering from Syracuse University. He holds three patents.

Patrick Hurley | is a computer engineer with the Air Force Research Laboratory's Information Directorate, Rome, NY. He holds a BS in computer science from the State University of New York at Oswego and a MS in computer science from the State University of New York Institute of Technology (SUNYIT). His research interests are in quality of service, cyber defense, survivability, and recovery.

Letter to the Editor

Q ***I know that organizations look favorably upon IA professionals who have earned industry-recognized certifications. The*** **IAnewsletter** ***has even published an article or two about the benefits of security certifications. Is there any indication that having employees with security certifications actually guarantees an organization better information security?***

A Having employees with a security certifications does help guarantee an organization a higher degree of preparedness, awareness, and readiness. Certifications provide a reasonable baseline by which to assess an individual's information assurance (IA) knowledge, so organizations with certified personnel are assured of having certain knowledge "on hand" should an information security incident occur.

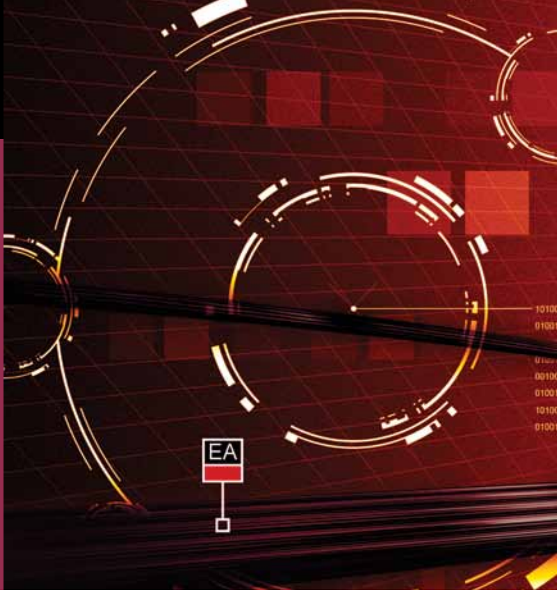
While the implementation and quality of security programs requiring certifications vary across organizations, significant information security requirements are levied on organizations, typically. For example, government organizations must meet requirements specified in the Federal Information Security Management Act, Department of Defense (DoD) and Intelligence Community directives, as well as internal Chief Information Officer policies. The IA community widely recognizes individuals with security certifications as also having sufficient technical knowledge to ensure these various security requirements are met.

Most importantly, organizations must prepare themselves to respond to unexpected information security incidents. Employing or having access to professionals with certifications, who can provide guidance to avoid vulnerabilities, diffuse threats, or appropriate responses to incidents, is a good risk management practice.

In summary, certifications are a reasonable indicator that an individual has certain IA knowledge. As a result, having certified personnel generally helps an organization achieve a higher degree of preparedness to respond to an information security incident.

For more information, DoD 8570.01-M has IA certification information that ties directly to DoD's Information Assurance Workforce Improvement Program: *http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf.*

Additionally, in the Fall 2009 edition of the *IAnewsletter*, W. Hord Tipton, the executive director of (ISC)^{2}, explains how the government benefits from requiring its key IA practitioners to earn industry-recognized certifications. You can read his article, "DoD Certifies the Power of Partnership," by visiting: *http://iac.dtic.mil/iatac/download/Vol12_No4.pdf*. ■



Upstream Security and Intelligence Case Studies

(Article 7 of 7)
by Tyson Macaulay

In this final article in our series on Upstream Intelligence (UI) and security, we will provide case studies about the successful application of upstream techniques to exposure assessment (EA). An EA is a combination of both a threat assessment and a vulnerability assessment, where the force and velocity of threats are measured and the degree to which vulnerabilities have been successfully exploited is observed. Unlike a typical vulnerability assessment, which estimates observed vulnerabilities and the potential for exploitation, an EA enumerates observed exploitations and allows for both known and unknown vulnerabilities to be triangulated.

An EA with its resulting, quantitatively derived security metrics are powerful applications of UI and security capabilities. The case studies we present in this paper are focused on EAs which have been performed at Bell Canada.

Outbound Messaging Analysis: Anonymous Organization

Upstream observations from messaging filtering infrastructure may reveal significant insights into the security posture and profile of a given organization based on messages leaving the organization. The anonymous organization maintains many independently managed messaging services and multiple Internet access points of presence. The population consisted of more than 30,000 e-mail users. Only messages traversing the Internet were included in the sample—intra-organizational messages were not observed. The sample was observed over the period of one month.

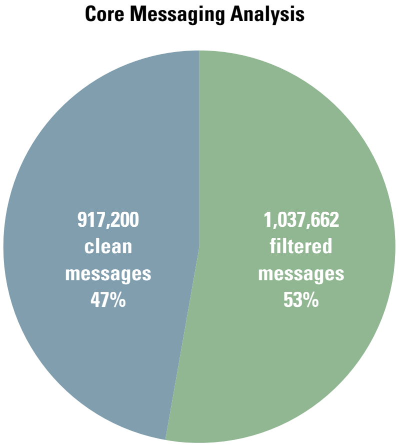


Figure 1 Upstream messaging analysis

As per Figure 1, more than one million messages in one month from the sampled domain were filtered due to problems associated with the suspicious sources, obvious spam, or viruses. Most of the filtered traffic (98%) was directly related to suspicious source rules, which flag previously observed spam generation or relay points and suspicious messaging patterns, among other factors. The remaining 2% of filtered traffic was due to spam or virus content within the message payload.

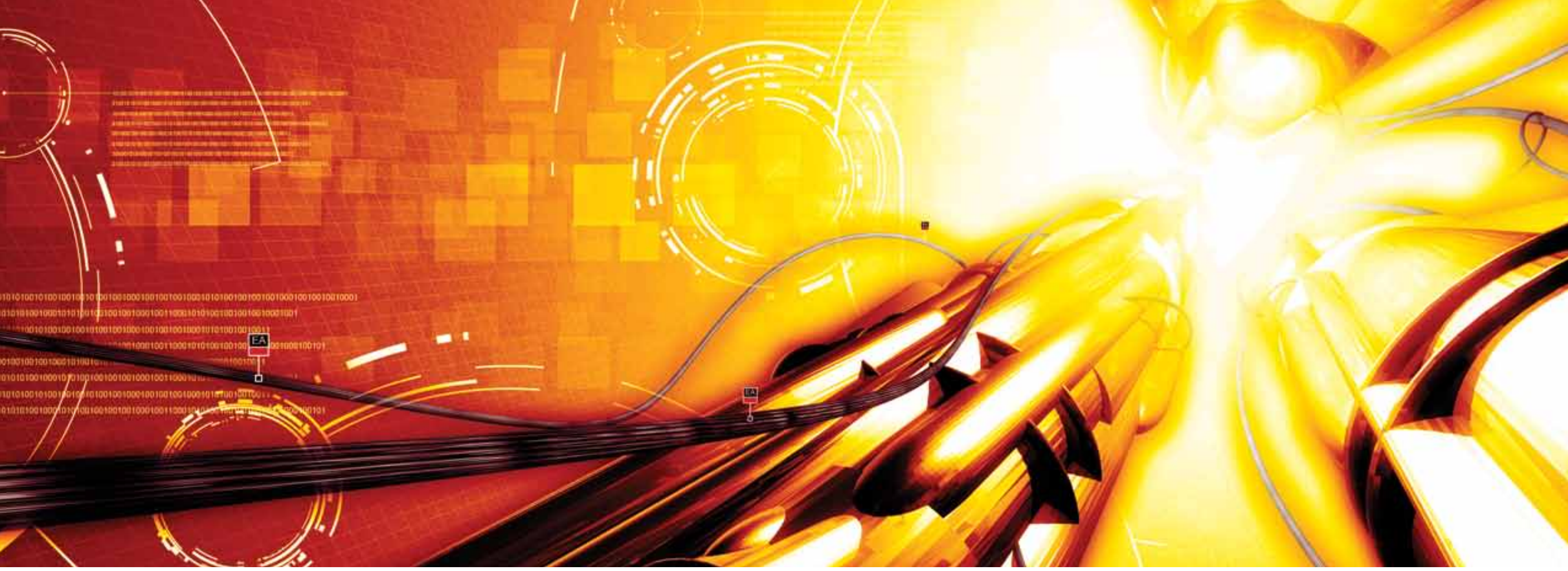
Many legitimate enterprises will experience some level of source filtering due to occasional mass mailings or inappropriate user behavior; however, this level of filtering is likely attributable to at least two factors: first, internal device compromise which impacts the e-mail-reputation of the organization and thus the ability to conduct business on the Internet; and second, that the organization's domain name is being widely forged (spoofed) for phishing attacks and poses a measurable threat to the organization's clients and its own reputation.

The 2% of spam messaging outbound from this organization is a significant indication of a compromised or "owned" device. While these messages have made it through the initial reputation filter (so the messaging server is considered to be reasonably trust-worthy), the second stage spam and virus filters are picking up and filtering out more bad messaging.

Botnet Command and Control Observations: Anonymous Organization

Upstream observations from carrier network management infrastructure may reveal insights into the security posture and profile of a given organization based on the patterns of apparently benign traffic heading to and from suspicious destinations.

Network analysis on traffic flowing to known, bad IP addresses and Autonomous System Numbers (ASNs) can indicate a security compromise in the form of a



command and control communications channel, without the need for any signature-based identification tools. The anonymous organization maintained multiple user gateways to the Internet. The population consisted of more than 5,000 internal Internet users. The sample was observed over the period of nine days, with sampling occurring up to four times a day for each sample day, during business and after business hours. The seed list of suspicious IP addresses and ASNs was compiled through a combination of open source and proprietary observations and consisted of several thousand cumulative IP addresses.

As per Figure 2, at any given time between 1.4% and 0.4% of sampled, bi-directional traffic flows are occurring with suspicious IP addresses and ASNs strongly associated with organized crime, state-sponsored intelligence, spamming, or all of the above. These traffic flows indicate that devices within the organization are communicating with untrusted domains. This is highly suspicious in nature and is a strong indicator of compromised devices inside the enterprise's domain. The total number of unique "flows" observed ranges from 22 to 53 at any given time in the sampled enterprise domain.

> Darkspace is like an unlit lightbulb—functional but not in use—hence the "dark" IP address "space"...Because malware frequently attempts to scan local networks for other devices to attack, it often blunders into darkspace.

Given the typical "active/dormant" cycles of botnets, the observations likely do not represent the entire population of compromised devices, only devices active during the sampling slots.

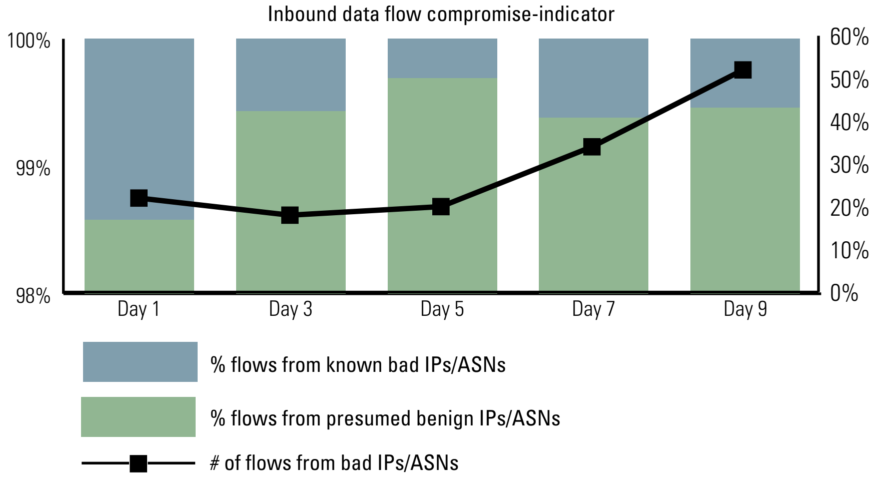


Figure 2 Inbound data flow compromise-indicator

Darkspace Observations Upstream

Darkspace is unassigned IP address-space. In some cases it may be legitimately routable on the Internet but has no machine associated with it. Darkspace is like an unlit lightbulb—functional but not in use—hence the "dark" IP address "space." Darkspace is frequently located adjacent to active IP space or IP addresses: numerically close by. Because malware frequently attempts to scan local networks for other devices to attack, it often blunders into darkspace. And because darkspace is unallocated, there are few reasons for legitimate traffic to find its way there other than rare user error.

Darkspace observations performed upstream allow for insight into the degree of threat positioned against an asset and the presence of compromised devices within an organization. Monitoring darkspace can be a useful and efficient input in the assessment of the level of

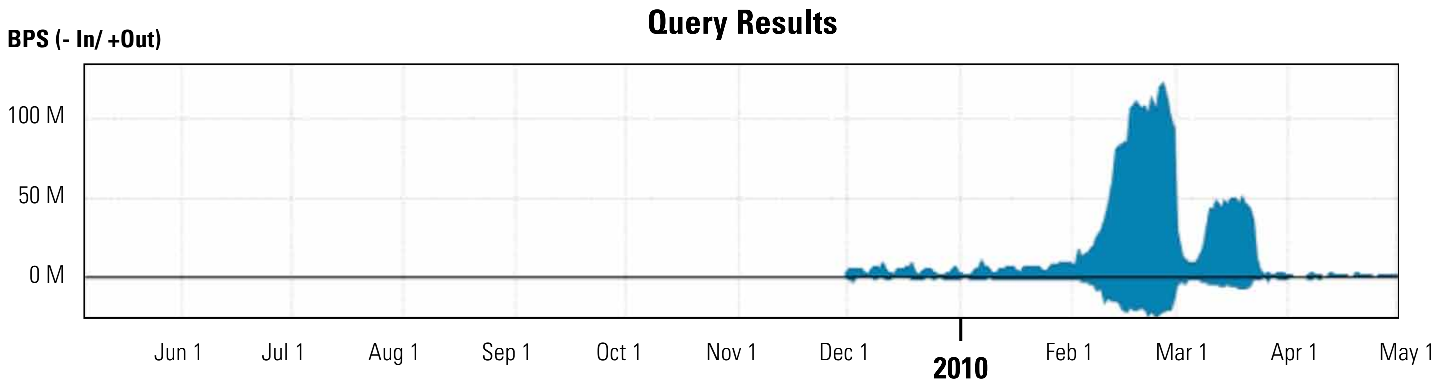


Figure 3 Olympic darkspace

threat against an asset. Monitoring darkspace can also be profoundly important to assessing the degree to which a network has been compromised by malware, especially on internal organization networks where the source is readily traceable.

Olympic Threat Measurement

Figure 3 shows upstream analysis of darkspace around the domains and address ranges used to provide an online presence for the 2010 Winter Olypmic games in Vancouver, Canada. These network connections not only provided support for the Olympic Web site and game results, but also provided Internet access for the myriad of athletes, coaches, media, Olympic Committee members, suppliers, and anyone else seeking Internet access from Olympic venues.

Readings above the horizontal-axis of the graph indicate traffic from darkspace destined for Olympic space. Since darkspace is by definition not in use, this traffic has therefore had its source address deliberately forged or "spoofed" so that it became unattributable. Traffic from darkspace is a very good indication of threat, since its purpose is either to probe defenses or inflict various forms of denial-of-service attacks. In the case of the 2010 Winter Olympics, a sustained assault of 100+ mbps of attack traffic was managed for the duration of the main event and 50 mbps for the duration of the Para-Olympics. In both cases, the online threat was real, measurable, persistent, and significant.

Readings below the horizontal axis indicate traffic from within the Olympic networks enroute to darkspace. This is a strong indication that devices utilizing the Internet connections supplied at the Olympic venues were compromised with malware. This is not necessarily surprising given the thousands of otherwise unrelated devices that were provided Internet access from the games. Within this cohort was enough malware to generate approximately 20 mbps of sustained traffic into darkspace, again indicating that the threat from inside the Olympic network perimeter also required management.

Critical Infrastructure Threat

Figure 4 shows upstream analysis of darkspace around critical infrastructure (CI) industries which are users of industrial control systems. For the purposes of this case study, several CI organizations from different sectors were anonymized and aggregated. While some of these industries may provide client services over the Internet, for the most part the Internet is not a critical hour-to-hour or even day-to-day part of the delivery of their goods and services.

Activity above the horizontal axis indicates that threats from darkspace related to probes and denial-of-service are rather limited. This indicates that these CI sectors do not (at least) appear to be the target of sustained, denial-of-service threats; however, other forms of persistent threat may certainly be targeting these industries through various phishing or "road apple" attacks (USB sticks loaded with

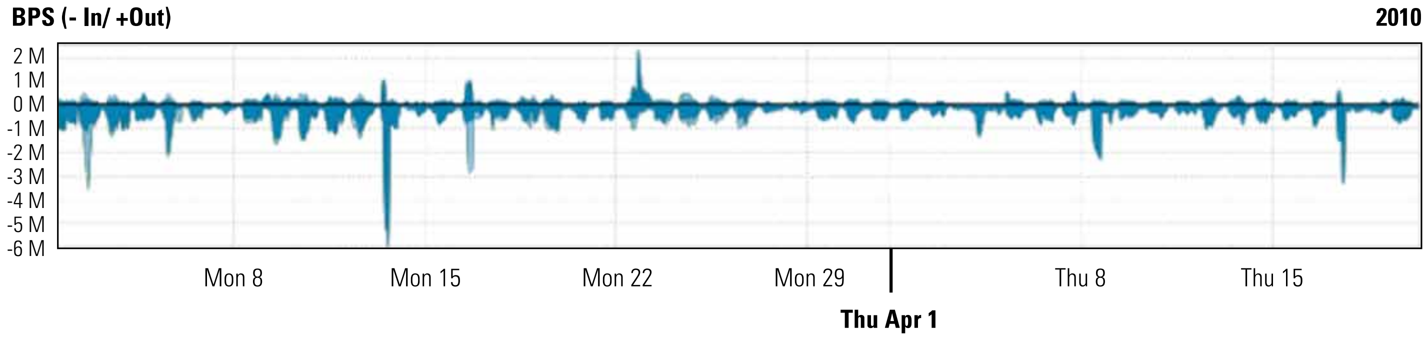


Figure 4 Critical Infrastructure darkspace

malware left in places where CI insiders might find them and attempt to use them—*a la* Stuxnet).

However, darkspace traffic observed below the horizontal axis indicates that some forms of attack other than denial-of-service have likely been successful. The darkspace traffic from CI appears to be coordinated with a typical working day, with traffic highest during working hours. A conclusion that could be drawn from these patterns may be that a significant proportion of the devices are either mobile devices (laptops) or non-critical systems that are powered off after the user leaves, as opposed to systems which would remain available around the clock. Similarly, the sometimes significant and repeated surges in darkspace traffic indicates that some level of detection and remediation is occurring, but this is not fully addressing the threat and not for long, indicating that more than one variant or instance of malware may be present.

Conclusions

This is the final article in our seven-part series spanning three issues of the *IAnewsletter*. The authors wish to thank IATAC for this opportunity to discuss upstream security and intelligence in unprecedented detail in front of such a distinguished audience.

While upstream is still very much in its infancy as a new layer of security, it is certainly the methodology representing the next hope for combating the relentlessly growing cyber threat. The infrastructure, methodologies, and precedents discussed in this series are merely the beginning for upstream security and intelligence capabilities. ■

About the Author

Tyson Macaulay | is the author and chief contributor for all seven Upstream Intelligence articles that have been featured in the Summer and Fall 2010 editions of the *IAnewsletter* as well as this edition. Tyson is also a member of IATAC's volunteer Subject Matter Expert program. We thank Tyson for introducing our readers to Upstream Intelligence and for his significant contributions to this publication and to IATAC as an information assurance center of excellence.

On behalf of the IAnewsletter*, thank you, Tyson, for your contributions.*
— The IAnewsletter *Editorial Board*

The 2011 Identity and Information Assurance (I&IA) Award

IATAC is pleased to promote the 2011 I&IA Award. This award will recognize military and civilian government personnel who significantly contributed to implementing the ASD/NII I&IA Strategy. Winners will be announced at the 2011 IA Symposium. Nominations are due 3 January. For more information, contact Mr. Mark Loepker at *mark.loepker@osd.mil.*

▷ *continued from page 23*

ASK THE EXPERT

your organization to begin assessing risk and what areas to focus on when doing a partner assessment. The formation of a tiger team with guidance from external experts is highly recommended when taking on the development of policy to drive major infrastructure decisions. ■

References

1. "Top Threats To Cloud Computing v1.0" report, Cloud Security Alliance, March 2010.

About the Author

Chris Silva | is the senior vice president of research and service delivery at IANS. In this role, Chris runs all daily operations of IANS' syndicated research and custom client advisory activities. Chris is committed to innovating the IANS research methodology to better serve security professionals. Chris comes from within the information technology research industry and is a veteran of several established research businesses. Chris served four-plus years at Forrester Research, most recently as a senior analyst working to serve security/risk and infrastructure/operations professionals. Chris is a graduate of the Isenberg School of Management at the University of Massachusetts.

The 2011 Information Assurance Symposium

The next IAS will be held in Nashville, TN, 7–10 March 2011. This well-attended conference is expected to fill up early. Watch the Web site *(http://www.informationassuranceexpo.com/)* for registration and agenda information. 2011 Identity and Information Assurance (I&IA) Award winners will be announced at this event.

2011 IA Symposium and IANS Mid-Atlantic Forum

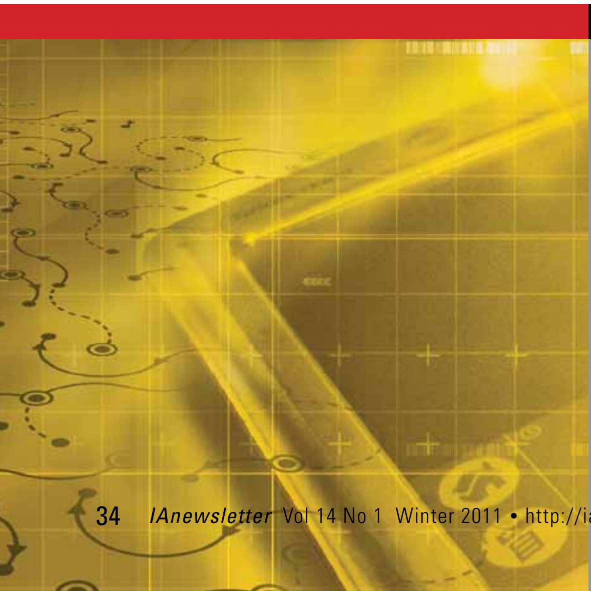
This year, two of IATAC's biggest conferences will take place during the second week in March: the 2011 DoD Information Assurance (IA) Symposium will take place 7–10 March 2011 at the newly restored Gaylord Hotel in Nashville, TN; the 2011 Institute for Applied Network Security (IANS) Mid-Atlantic Information Security Forum will take place 8–9 March 2011 at the JW Marriott in Washington, DC. Both of these conferences provide participants with critical information on how IA is evolving, and they allow participants the opportunity to collaborate in developing innovative solutions that will propel IA forward.

The IA Symposium is the biggest conference IATAC attends each year. It attracts around 2,000 IA professionals from government, industry, and academia, allowing attendees the opportunity to network and learn more about IA policy, governance, and technology through hands-on training and nearly 100 different presentations.

At this year's symposium, the office of the Assistant Secretary of Defense for Networks & Information Integration (ASD/NII) will present the 2011 Identity and Information Assurance (I&IA) Award. This award recognizes military and civilian government personnel who significantly contributed to implementing the ASD/NII I&IA Strategy. Award submissions are due 3 January 2011. For more information about this award and how to submit nominations, please visit IATAC's Web site, *http://iac.dtic.mil/iatac/.*

The 2011 IANS Mid-Atlantic Information Security Forum will bring experienced IA and Information Technology (IT) professionals together to share information about the industry's most pressing issues. This forum is a unique event because attendees get to participate in peer-to-peer technical and strategic discussions about how to address critical IA and IT problems. Each year, IATAC helps lead some of these roundtable discussions, and IATAC subject matter experts deliver presentations on various IA topics.

We look forward to attending and participating in both the IAS and IANS Mid-Atlantic Information Security Forum in 2011. For more information about IAS, please visit *https://www.globreg.com/IAE2011/.* For more information about the IANS Mid-Atlantic Information Security Forum, please visit *http://www.iansresearch.com/forums/calendar.html.* ■



The Security Risk Management for the Off-the-Shelf Information and Communications Technology Supply Chain State-of-the-Art Report (SOAR) Now Available!

IATAC is proud to release the Security Risk Management for the Off-the-Shelf Information and Communications Technology Supply Chain State-of-the-Art Report (SOAR). This SOAR has limited distribution. For more information or to request a copy, please e-mail *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 before 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 ______________________________

Organization ______________________________

Address ______________________________

____

____

DTIC User Code ______________________________

Ofc. Symbol ______________________________

Phone ______________________________

E-mail ______________________________

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 □ **Firewalls** □ **Intrusion Detection** □ **Vulnerability Analysis** □ **Malware**

Critical Review and Technology Assessment (CR/TA) Reports

□ Biometrics (soft copy only)
□ Data Mining (soft copy only)
□ Wireless Wide Area Network (WWAN) Security
□ Configuration Management (soft copy only)
□ IA Metrics (soft copy only)
□ Defense in Depth (soft copy only)
□ Network Centric Warfare (soft copy only)
□ 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)

□ Security Risk Management for the Off-the-Shelf Information and Communications Technology Supply Chain (DTIC user code must be supplied before these reports will be shipped)
□ Measuring Cyber Security and Information Assurance
□ The Insider Threat to Information Systems (DTIC user code must be supplied before these reports will be shipped)
□ A Comprehensive Review of Common Needs and Capability Gaps
□ Software Security Assurance
□ IO/IA Visualization Technologies (soft copy only)
□ Modeling & Simulation for IA (soft copy only)
□ Malicious Code (soft copy only)
□ Data Embedding for IA (soft copy only)

UNLIMITED DISTRIBUTION

IAnewsletters hardcopies are available to order. Softcopy back issues are available for download at *http://iac.dtic.mil/iatac/IA_newsletter.html*

Volumes 12	□ No. 1	□ No. 2	□ No. 3	□ No. 4
Volumes 13	□ No. 1	□ No. 2	□ No. 3	□ No. 4
Volumes 14	□ No. 1			

SOFTCOPY DISTRIBUTION

The following are available by e-mail distribution:

□ IADigest
□ IA/IO Scheduler
□ Research Update
□ Technical Inquiries Production Report (TIPR)
□ IA Policy Chart Update

Fax completed form to IATAC at 703/984-0773

IATAC

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

Calendar

January

Blackhat DC 2010
16–19 January 2011,
Arlington, VA
http://www.blackhat.com/index.html

US DoD Cyber Crime Conference 2011
21–28 January 2011
Atlanta, GA
http://www.dodcybercrime.com/11CC/index.asp

ShmooCon
28–30 January 2011
Washington, DC
http://www.shmoocon.org/

February

RSA Conference
14–18 February 2011
San Francisco, CA
http://www.rsaconference.com/2011/usa/index.htm

AFCEA Homeland Security Conference
22–24 February 2011
Washington, DC
http://www.afcea.org/events/homeland/10/home.asp

March

DoD IA Symposium
7–10 March 2011
Nashville, TN
http://www.informationassuranceexpo.com/

IANS Mid-Atlantic Information Security Forum
8–9 March 2011
Washington, DC
http://www.iansresearch.com/forums/calendar.html

IAPP Global Privacy Summit
9–11 March 2011
Washington, DC
https://www.privacyassociation.org/events_and_programs/global_privacy_summit/

2011 Information Management Conference
21–25 March 2011
Las Vegas, NV
http://doeimc.energy.gov/11EI/index.asp

AFCEA Belvoir Industry Day
29–30 March 2011
National Harbor, MD
http://www.afceabelvoir.org/industryday.aspx

SANS 2011
28 March– 4 April 2011
Orlando, FL
http://www.sans.org/sans-2011/

April

2011 DTIC Conference
4–6 April 2011
Alexandria, VA
http://www.dtic.mil/dtic/announcements/conference.html

2011 DoD Enterprise Architecture Conference
11–15 April 2011
Hampton, VA
http://www.afei.org/events/1A05/Pages/default.aspx

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