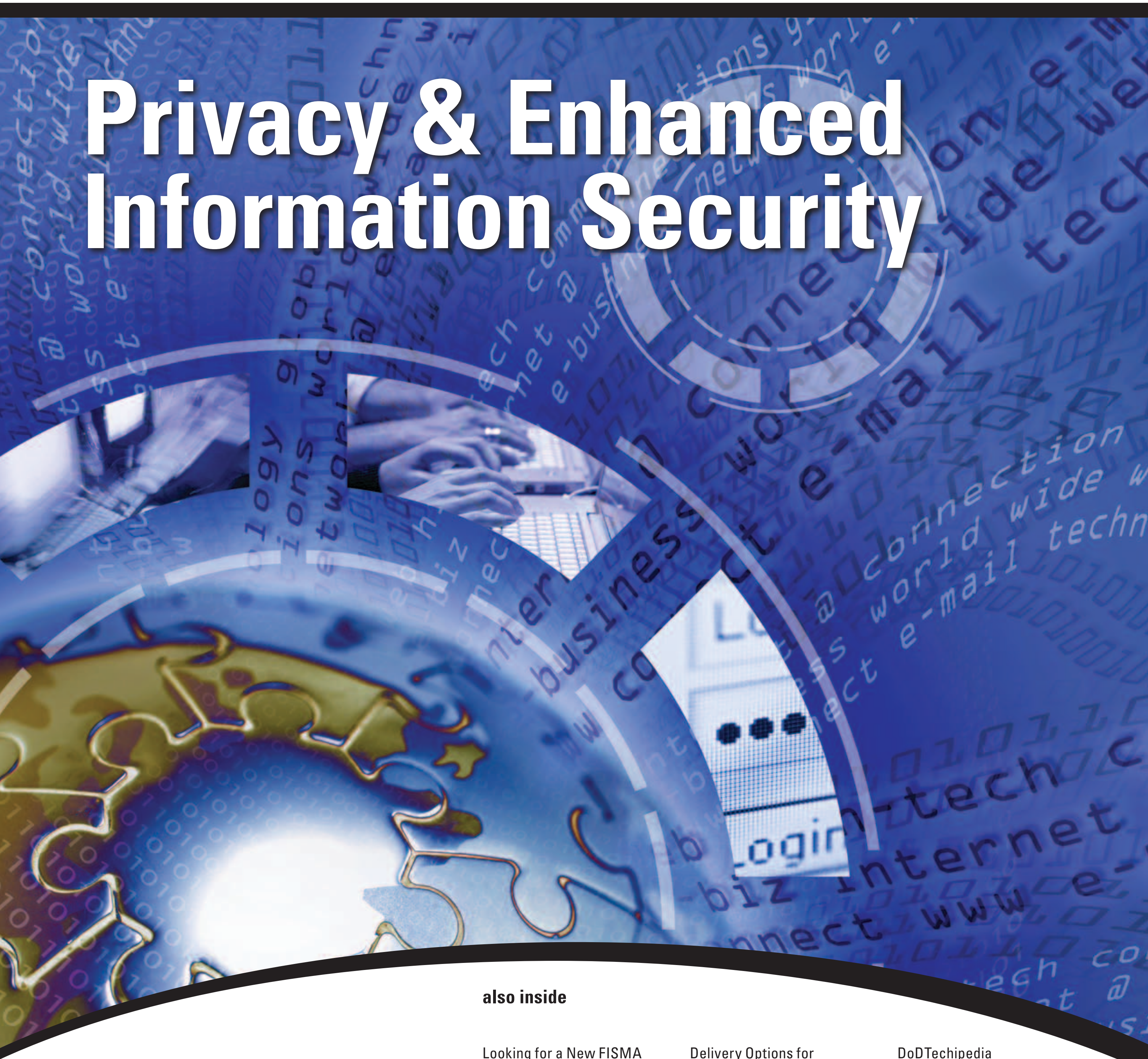
13/4

Volume 13 Number 4 • **Fall 2010**

IAnewsletter

The Newsletter for Information Assurance Technology Professionals

Privacy & Enhanced Information Security



also inside

IATAC

contents

DDRE

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: Michelle DePrenger
Copy Editor: Daniel Eckroad
Editorial Board: Al Arnold
Angela Orebaugh
Dr. Ronald Ritchey
Designers: Dustin Hurt
Kacy Littlehale
Brandi Samchisen
Kali Wilson

***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: Donald Rowe
Newsletter design: Donald Rowe

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

in every issue

IATAC Chat

Gene Tyler, IATAC Director

Well, much has happened since we last "chatted" and in this edition I have lots of exciting news. While compiling this edition of the *IAnewsletter*, we received some breaking information regarding upcoming IA events. IATAC tracks important conferences, workshops, symposiums, and training events. Our IA/IO Events Scheduler highlights these types of activities and I recommend you visit our website *(http://iac.dtic.mil/iatac)* to learn more and to stay connected. Now for some specifics:

- **2011 IA Symposium:** The IA Symposium, which is traditionally held in February, will take place 7–10 March 2011. It will be held at the Gaylord Hotel in Nashville, TN. Registration opens in December. As a part of the Symposium, the annual 2011 Identity and Information Assurance (I&IA) Award winners will be announced. ASD/NII will recognize military and civilian government personnel who significantly contributed to implementing the ASD/NII I&IA Strategy. Award submissions are due 3 January 2011. Go to the IATAC website for more information.
- **2011 IANS Mid-Atlantic Information Security Forum:** The Institute for Applied Network Security will hold its Mid-Atlantic Forum 8–9 March 2011 at the JW Marriott in Washington DC. I highly encourage you to consider attending this forum as IATAC will collaborate with IANS for this event. Go to either IATAC's or the IANS' website *(www.iansresearch.com)* for more information.

In addition to these IA events, I want to highlight our latest State-of-the-Art Report (SOAR). We have been talking about releasing our Supply Chain SOAR for nearly a year, and I am happy to announce its official release! IATAC subject matter experts and IATAC's Steering Committee agreed that supply chain security is a critical topic area in need of greater attention. In order to provide our IA community with more information, IATAC published our newest SOAR, titled *Security Risk Management for the Off-the-Shelf Information and Communications Technology Supply Chain.* It was released in August and is posted on our website. This SOAR has limited distribution, so to obtain a copy, please register with DTIC at *http://www.dtic.mil/dtic/registration/.* Your DTIC registration will not only allow you to obtain our SOAR, but it will also enable you to access a wide variety of other IATAC and DTIC information.

As I always say, inside this edition we have something for everyone. For individuals like me who believe privacy and IA cannot really be separated, I invite you to check out "Work Place Privacy." Our government security professionals will be interested in "Looking for a New FISMA." We also have a collection of articles on the Air Force Institute of Technology. AFIT nearly always contributes articles to the *IAnewsletter*. I challenge any other institution to follow AFIT's lead because we are waiting to hear from you!

On one final note, in August, Secretary of Defense Robert Gates announced that there will be some changes in the future. These changes will most likely impact the IA functions within DoD now managed by OASD(NII), the Joint Staff J6, and Joint Forces Command. We do not know the results of these changes, but as information is released we will help pass on the news. Stay plugged in—there will be more to come.

As always, I encourage our readers to contact IATAC with questions or ideas about how we can better serve you. Thank you for your continued support, and we look forward to seeing you at the IAS and the IANS Security Forum.

Gene Tyler

The 2011 Identity and Information Assurance (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, visit *http://iac.dtic.mil/iatac.*

Looking for a New FISMA

by Chris Merritt

The Federal Information Security Management Act (FISMA) of 2002 was authored with good intentions, but has endured very poor execution. It's a generally well known fact that FISMA has had many critics over the years that accuse the law of focusing more on documentation than actual implementation of security practices within the federal space—including the Department of Defense (DoD). Within the DoD alone, the law has been responsible for the creation of volumes and volumes of documentation—much of which is obsolete or outdated by the time it is published and approved as part of the certification and accreditation (C&A) process. In recent testimony to Congress, Vivek Kundra, Federal Chief Information Officer, Administrator for e-Government and Information Technology Office of Management and Budget, wrote that, "… over the last six years, the Department of State spent $133 million amassing a total of 50 shelf feet, or 95 thousand pages, of documentation for about 150 major IT systems." He then referred to these pages as "paper snapshots." [1]

The transition from the DoD Information Technology C&A Process (DITSCAP) to the DoD Information Assurance C&A Process (DIACAP) several years ago has alleviated a lot of the over-burdensome documentation requirements. And thankfully, the security posture of enclaves or information systems is no longer inferred from how thick the DITSCAP binder is. In the past, the thicker the DITSCAP binder, the more secure the system was thought to be!

DIACAP solved a lot of this misconception by focusing less on documentation and more on the implementation of security controls. However, there is still a long way to go, and the focus remains on compliance instead of performance. This article will identify the two fundamental issues with existing compliance processes that comprise the majority of FISMA scoring, and will highlight some ongoing efforts to reshape FISMA in 2010.

Performance vs. Compliance: Securing Well or Scoring Well?

The first question to ask is, *are you more interested in securing your infrastructure and systems or getting a good FISMA score?* These two goals aren't always mutually exclusive, but they can be more often than not. The number one, fundamental flaw I (and many others) see in FISMA, is that the focus is primarily on whether or not you have a control in place —instead of the effectiveness of that control. Here are two examples:

First, DoD policy requires a continuity of operations test to be conducted annually for information systems and enclaves. This is one of the controls in DoD Instruction (DoDI) 8500.2. I've seen instances where, during a C&A effort, an information system was given a compliant score for this control because the system manager had conducted a continuity test that year, even though that test failed miserably. I've also seen an overwhelming use of so-called table-top continuity tests that allow system managers to state that their system's continuity of operations was tested. The system managers, however, still have no idea how the system would fare if their system or the critical infrastructure it relies on became unavailable for any reason. This of course jeopardizes the security posture of the organization and more specifically, the mission that the information system or enclave supports.

Second, monthly vulnerability scanning of information systems is also a requirement and certainly a best practice given the volume of patches that are released weekly and the volatility in technology today. As part of C&A validation teams, I have seen many organizations happy to proclaim that they are scanning monthly. But when you dig a little deeper, you quickly learn that nobody is reviewing the results of the scans.

In the two examples above, do the system or enclave managers meet the letter of the FISMA Law? Yes. Is the security posture of the organization or its mission positively impacted by these efforts? Absolutely not. The final product with respect to the two controls above is the appearance that all is well, when in fact, it's quite the opposite.

Because of the focus on *do you have it?* instead of *how well does it work?*, it's not very difficult to manipulate the FISMA process for a solid grade of A or B. Doing so provides a false sense of security, and makes organizations within the federal

Hopefully, Congress will get FISMA 2.0 right by ensuring the new law focuses more on performance, and less on compliance.

government unnecessarily vulnerable. If organizations choose to look a level deeper and perform assessments geared at assessing effectiveness, their FISMA scores will almost certainly suffer. This incentivizes organizations to review their systems and enclaves according to the letter of the law and focus on what they have instead of how well it works.

The good news is that FISMA reporting in 2010 is changing. Office of Management and Budget (OMB) is going to begin looking more closely at spending habits of federal organizations to get a better understanding of the correlation between government spending and the performance impact of security dollars. Again, the shift seems to be moving away from compliance efforts (do you have it—yes or no?) into performance-based metrics that describe how well those compliance efforts are working.

In his written testimony to Congress, Kundra outlines several in-progress initiatives that are designed to proliferate some of the new goals attached to proposed FISMA law amendments. Some of these programs include:

- A new focus on coordination with the Cybersecurity Coordinator leading the way and involving the private sector and the Comprehensive National Cybersecurity Initiative (CNCI)
- Shifting to performance-based culture by proliferating White House aspirations of transparency through TechStat, implementing continuous monitoring, managing and analyzing information security costs, and new centralized reporting capabilities such as CyberScope
- Taking an enterprise approach to managing cybersecurity by establishing standards such as the Federal Desktop Core Configuration and the Trusted Internet Connections initiative, putting more emphasis on awareness and cybersecurity education and training, leveraging federal purchasing power through the use of Blanket Purchase Agreements, implementing Federal Identify Management initiatives like HSPD-12
- Developing more robust research and development plans by enhancing the relationship between the government and the private sector (*e.g.,* The Special Cyber Operations Research and Engineering [SCORE]).

Hopefully, Congress will get FISMA 2.0 right by ensuring the new law focuses more on performance, and less on compliance. Anything less than metrics based on performance will ensure that organizations continue spending millions of dollars complying instead of actually securing the federal infrastructure.

Information Security Controls—All or Nothing?

John Gilligan, the former Air Force Chief Information Officer, illuminates the second fundamental issue with FISMA in his recent testimony to Congress. He also notes that FISMA was a positive step towards securing our federal infrastructure, and that it has some positive elements, but that the overall approach is flawed. The primary example he provides is that FISMA does not focus on a small subset of security controls that have the greatest impact on information security. Instead, FISMA requires organizations to implement, "…the entire catalog of controls (over 300 separate controls) published by the National Institute of Standards and Technology (NIST)." For DoD, it's somewhere in the neighborhood of 150 controls to align with DoDI 8500.2 (however, the Department is looking at the possibility of abandoning DoDI 8500.2 for NIST SP 800-53).

This approach has caused organizations to perform at sub-par levels in their attempts to get something in place to satisfy a control or requirement—even if that something is insufficient or not effective. Again, this is the approach of being able to check a box, and not worry about how well something performs. Also, implementing every control

Control	Automatable
Inventory of Authorized and Unauthorized Devices	Yes
Inventory of Authorized and Unauthorized Software	Yes
Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Yes
Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Yes
Boundary Defense	Yes
Maintenance, Monitoring, and Analysis of Audit Logs	Yes
Application Software Security	Yes
Controlled Use of Administrative Privileges	Yes
Controlled Access Based on Need to Know	Yes
Continuous Vulnerability Assessment and Remediation	Yes
Account Monitoring and Control	Yes
Malware Defenses	Yes
Limitation and Control of Network Ports, Protocols, and Services	Yes
Wireless Device Control	Yes
Data Loss Prevention	Yes
Secure Network Engineering	No
Penetration Testing and Red Team Exercises	No
Incident Response Capability	No
Data Recovery Capability	No
Security Skills Assessment and Appropriate Training to Fill Gaps	No

Table 1 Top 20 Controls Recommended by the CAG [2]

in the catalog is simply not feasible for very large, global federal organizations with tight budget restrictions or insufficient resources.

To remedy this problem, a consortium of information security experts from government and the private sector came together to develop a new compliance vertical. This new cornerstone of compliance and performance is known as the *Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG),* and was released in late 2009.

The CAG takes the approach of identifying the 20 most critical information security controls that, if addressed properly, will mitigate risk associated with a large percentage of threats faced by Federal IT. What is great about these top 20 is that 15 of them are automatable. The top 20 controls recommended by the CAG are listed in Table 1.

For each control, the CAG provides a description about how attackers exploit the lack of the control, how the control can be implemented to include quick win scenarios, mapping to NIST controls, procedures and tools for implementing the control, metrics for measuring compliance and performance of the control, and testing procedures.

For organizations struggling with compliance with FISMA, or for those that already have a good grade in FISMA that may be based on compliance rather than performance, I highly recommend reviewing the CAG. Perform an audit based on the performance measures defined in the CAG to get a good idea of how well your information security controls fare against performance-based criteria—which will hopefully be the future foundation of FISMA 2.0.

Conclusion and Further Reading

If you are unfamiliar with the new efforts to modify FISMA or the CAG, I highly recommend further research, as my description here is merely the tip of the iceberg. Many information security professionals within the federal space are excited about adjustments to the FISMA metrics and the law itself, but some claim that drafts of the new law are not different enough, and may actually hurt future cybersecurity efforts. I recommend doing the research and forming your own opinion. The best time to affect change is before it's implemented. Either way, be prepared for change in the coming months and years as the federal government attempts to get better at managing and affecting information security.

More information and additional reading on these topics can be found here:

- **Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG)—***http://www.sans.org/critical-security-controls/*
- **Testimony to Congress regarding FISMA—***http://www.sans.org/newsletters/newsbites/newsbites.php?vol=12&issue=24#sID200*
- **Draft Proposed Law has limited release—**Look for: H.R.4900—Federal Information Security Amendments Act of 2010
- **Measuring Cybersecurity and Information Assurance—**IATAC's State-of-the-Art Report that assesses real-time, accurate IA measurement ■

About the Author

Chris Merritt | is the CEO of Prolific Solutions, LLC (*www.prolific-solutions.net*) and has been consulting for the DoD for over eight years. He is the author of proVM Auditor (*www.provmauditor.com*), a vulnerability assessment aggregation and compilation tool, and holds a number of information security certifications, including CISSP and CISA. He earned his Master's degree in information assurance from Norwich University in 2007.

References

1. *http://oversight.house.gov/images/stories/Hearings/Government_Management/032410_Federal_Info_Security/2010.* FISMA. Kundra.testimony.final.pdf
2. *www.sans.org/critical-security-controls/*

Enterprise Client Research Encryption

by Chris Silva

In this installment of Ask The Expert, we'll address how best to mitigate third-party risk by taking a deep dive into one such area—key management. In addition to traditional advice, such as encryption keys not being revealed to third parties (*i.e.,* contractors, service providers, partners, or other vendors) without approval of a Global Information Security Officer, and all encryption keys being protected by technical or procedural controls reviewed and approved by a Global Information Security Officer, the following is a list of encryption key management best practices:

- The same encryption keys must not be utilized for multiple different devices (*e.g.,* blindly reproducing keys as part of a golden image or part of an automated build/install script).
- Application keys must not be treated as source code.
- Encryption Keys must be treated as confidential, especially with regard to shipping/transferring. (*i.e.,* users should not ship keys with passwords, or store them on electronic storage media in combination with password document in or on the media).
- Encryption keys must only be issued with proper identification and authorization. Users must validate that the requestor has authority to issue keys. Examples of proper identification include validation of a government-issued photo ID; examples of proper authorization include written acknowledgement from an organizational representative.
- Developers must be restricted from developing in-house key management systems or encryption algorithms and may only use approved solutions and architectures.
- Strong passwords must be used for key export files (*e.g.,* P12 files or certificate backups).
- Escrowed keys, archived keys, and key recovery systems must be validated and tested at least annually.
- Employees should be required to seek written approval before installing and activating non-standard cryptographic solutions (*i.e.,* file, laptop, or e-mail encryption solutions not installed as part of a default desktop, server image, or installed as part of an approved application package).
- Encryption keys must not be hardcoded into software, source code, or scripts, particularly on .jsp, .aspx, or .php files.
- New developments and implementations must not be allowed to utilize deprecated encryption solutions (*e.g.,* DES for new applications.)
- Developers of in-house applications using cryptographic functionality should be required to ensure cryptographically-secure storage of encryption keys.
- Developers of in-house applications using cryptographic functionality must be required to "scrub" any media storing temporary keys (*e.g.,* session keys), "zeroize" memory buffers used to store plaintext private or secret keys, and lock memory pages containing plaintext private or secret keys.
- All encryption keys (including keys in development environments) must follow production requirements (password, length, algorithms, *etc.*) All keys must use the full keyspace allowed (for example, not limiting key buffers to printable characters).
- When Litigation Hold requirements are lifted the encryption keys for the scoped data need to be deleted as directed by Legal (assuming no other retention requirements are impacted). ■

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.

Securing Telework and Remote Delivery of Dispersed Teams

by Brian J. Bates

> With all of the notoriety and discussion that telework, remote delivery, and dispersed teams receive, security is not commonly thought about as much as other topics.

Perhaps you know of or work with someone who is delivering support from a remote or telework location. Perhaps you are delivering remotely or are the manager of a dispersed team. This type of working arrangement is very common in today's business environment and organizational structure. As desired or required skills are distributed globally, technology is an enabler, and work-life balance is more important than ever. This model for dispersed teams is only going to evolve further into the typical team structure. In June 2008, the House of Representatives voted to require federal agencies to expand telecommuting. Forty-one percent of federal employees are eligible to work remotely, however, only 19% do so. Forty-two percent of US companies now say they have a telework program, up from 30% in 2007. [1] Given the Defense Base Realignment and Closure (BRAC), skilled employees may exist to satisfy a business or organizational need in one geographic location, but are rooted in another location. With all of the notoriety and discussion that telework, remote delivery, and dispersed teams receive, security is not commonly thought about as much as other topics (benefits, policy, communication, implementation, work assignments, *etc.*). Security is typically an afterthought and often difficult to establish, monitor, maintain, and enhance with dispersed teams.

The remainder of this article will focus on four (4) challenges, or "opportunities," that exist with securing telework and remote delivery. A discussion of lessons learned, tips, and steps for implementing several key actions are also included.

So, what are the overarching challenges/opportunities? Understanding and willingness to break away from the traditional workplace mold and realizing that the required/desired skills are not always in the same geographic location is the major hurdle. Equally important is the ability to proficiently manage and monitor remote resources and dispersed teams; achieving this with a focus on security will help yield success *via* remote delivery. If you or your team are new to this type of model or your dispersed team is looking to mature, continually emphasizing the points below will give you a solid foundation for managing your entire team with a focus on security.

Managing Telework and Remote Delivery Resources

The first major challenge involves knowing your organization and your people. If you don't know your business or employees, how can you identify and manage resources, let alone the remote team members? Who is on your team, what are they capable of or interested in, and do they know you? Are your team's objectives/goals well written, published, measurable, and achievable? Does your team follow the same sheet of music or game plan? These are all questions you should ask in order to manage your dispersed team. The following actions should be considered to prepare your team for success:

- Take inventory of your business clients and services offered. Know what is acceptable and what can change. Identify gaps in policy, process, and technology.
- Take inventory of your team's skills and interests. Understand where the gaps are and hire or train personnel to address them.
- Dispersed teams need context to work by. Your team needs to know about you, your goals, and your preferences. Publish team goals and plans regularly. If possible, socialize, collaborate, and obtain concurrence from team members.

- Dispersed teams also need a construct to operate within. Know what is acceptable and preferred. Understand and establish the basic rules. Don't be afraid to improvise.
- From a security perspective, the fundamental objectives for telework and remote access technologies are as follows: *Confidentiality*—ensure that remote access communications and stored user data cannot be read by unauthorized parties. *Integrity*—detect any intentional or unintentional changes to remote access communications that occur in transit. *Availability*—ensure that users can remotely access resources whenever needed.

Physical and Cyber Controls

Issues arising from the next two challenges are largely preventable. Breeches in physical or cyber security due to improper security controls or a lack thereof is a major concern for dispersed teams. Client devices are used in a variety of locations, such as employee homes, coffee shops, hotels, and conferences. The mobile nature of these devices makes them likely to be accessed, lost, or stolen, which places the data on the devices at increased risk of compromise. The following mitigation strategy can help protect you and your dispersed team:

- When planning telework security policies and controls, assume that client devices will be acquired by malicious parties who will attempt to recover sensitive data from the devices.
- Encrypt the client device's storage so that sensitive data cannot be recovered from it by unauthorized parties.
- Another option is not storing sensitive data on these remote client devices.
- Plan your security controls accordingly by assuming that client devices will become infected. Use appropriate anti-malware technologies from the organization's secure configuration baseline, such as anti-malware software on client devices.
- Consider the use of network access control (NAC) solutions that verify the security posture of a client device before allowing it to connect to an internal network.
- Consider using a separate network for telework client devices, instead of permitting them to directly connect to the internal network.

Remote Access and Remote Delivery Behaviors

Even with the best security controls in place, people still find a way to circumvent them or practice "bad security." An infected machine on a secure network can still occur due to inappropriate remote access behaviors. Remote access provides external hosts with access to internal resources, such as servers. With unsecured networks, organizations normally have no control over the security of the external networks used by telework/remote delivery clients (*e.g.,* home networks, hot spots). Each potential form of remote access significantly increases the risk of the internal resource being compromised and exposes the resource to new threats, particularly from untrusted client devices and networks. Communications systems used for remote access (*e.g.,* telephone, DSL, broadband, *etc.*) are susceptible to eavesdropping, which places sensitive information transmitted during remote access at risk of compromise. Man-in-the-middle attacks may also be performed to intercept and modify communications. The following actions can help you mitigate these risks:

- Develop a remote access security plan based on the assumption that the networks between the telework client device and the organization, including teleworkers' home networks, cannot be trusted.
- Risks from use of unsecured networks can be mitigated, but not eliminated, by using federally approved encryption technologies to protect the confidentiality and integrity of communications, as well as using mutual authentication mechanisms to verify the identities of both endpoints.
- Carefully consider the balance between the benefits of providing remote access to additional resources and the potential impact of a compromise of those resources.

- Ensure that any internal resources made available through remote access are hardened appropriately against external threats, and that access to the resources is limited to the minimum necessary through firewalling and other access control mechanisms.
- Strive for excellence and transparency. Opportunities flagged as low risk/low reward are less susceptible to targeted attacks. Also, if remote resources keep their visibility low or private, the risk of being targeted is reduced.

Monitoring, Change, and Awareness Refreshers

Lastly, don't forget to monitor security within and across your dispersed team. Do not assume your team is practicing "good security." A lack of interest to raise and/or obtain awareness and understanding of security may exist and go unnoticed or unaddressed. In addition to the tips below, understanding that policies, people, and technologies change can drive your team to focus on monitoring for incidents and change: [2]

- Verify all new employees and contractors have received and signed rules of behavior prior to receiving system access.
- Ensure that users who have a need for remote access receive appropriate training and support.
- Ensure initial/new user security awareness training is provided for new employees and contractors.
- Ensure refresher user security awareness training is conducted and attended.
- Be comfortable with the fact that you and your team will change and build change into your team's goals.
- Know the basics and protect you and your team. "Be there" for your virtual team. Operate in a proactive and open manner.
- Identify and report events before they become incidents. Know what to do and who to leverage based on the severity of an event.
- Adjust your style and enhance your skills. Monitor and manage to plans and results. Skills training in areas of time management and organization will provide you with more time for monitoring and communicating with your team; "Getting things Done" and "Getting to inbox zero." [3]

So, what actions could a remote employee or manager of a dispersed team take to begin implementing secure remote delivery or management? Common topics that are instrumental in setting up a successful and secure dispersed team environment include strategy, tools, data, personnel, and physical security. For more on these points, see the details in the General Services Administration article published in July 2009 entitled, "Meeting Security Perils of Telework and Alternative Work Arrangements." [4] Other specific actions include:

- **Creating a Team Plan/Charter**—This is the first step in building a successful team. It contains the context, mission and objectives, composition and roles, authority and boundaries, resources and support, operations, negotiation, and agreement.
- **Creating a Communications Plan**—Be the Chief Communications Officer (CCO) for your team.

Phase	Actions
Initiation Phase	▶ Identify needs for telework and remote access/delivery. ▶ Provide an overall vision for how remote access solutions would support the mission of the organization. ▶ Create a high-level strategy for implementing remote access solutions. ▶ Develop a telework/remote delivery policy, guidance and process for access, and specify business and functional requirements for the solution. ▶ Create formal telework/remote delivery agreements.
Development Phase	▶ Specify the authentication methods, the cryptographic mechanisms used to protect communications, firewalls and other mechanisms used to control access to networks and resources on those networks. ▶ Provide appropriate training and support. ▶ Research client needs since they can affect the desired policies. ▶ Ensure that the security policy can be employed and enforced by all clients. ▶ Procure all components needed for the solution.
Implementation Phase	▶ Document telework security policy in the system security plan and/or your team charter. ▶ Install and test a proof of concept or pilot for telework/remote delivery, then activate it on a production network. ▶ Monitor security using the configuration of other security controls and technologies, such as security event logging, network management, and authentication server integration.
Operations and Maintenance Phase	▶ Once the solution is operational, perform security-related tasks on an ongoing basis, such as monitoring, assessments, surveys, and refresher training. ▶ Perform log review and attack detection. These tasks should be documented in the configuration management plan. ▶ Ensure automatic pushes for updates/patches and monitoring and tracking of data, rights, and hardware that telework/remote access users can access. ▶ Communicate progress and results. ▶ Leverage telework/remote delivery for continuity of operations.
Disposal Phase	▶ Conduct these tasks when a remote access solution or its components are being retired: • Collection of data and hardware • Cancellation of rights and access • Termination of connectivity • Preserving information to meet legal requirements • Sanitizing media; and • Disposing of equipment properly.

Table 1 Security Life Cycle Tips

- **Technology**—Leverage technology consistently and be proficient.
- **Organization**—Be available and organized. Manage schedules and milestones rather than letting them manage you.
- **Run your team like a project or program**—Set, plan, design, execute, monitor, and adjust your objectives and goals.

Another alternative to implementing secure remote delivery is to think in terms of a security life cycle—Initiation, Development, Implementation, Operations and Maintenance, and Disposal—to achieve success with a dispersed team. Table 1 contains some final tips to consider.

In closing, securing people, information, and physical assets takes work, awareness, and dedication to be successful. There is no doubt that maintaining a secure, dispersed team environment presents many unique challenges. These challenges can be managed, and many organizations have embraced this team structure and have been providing secure remote access programs for years. These organizations have identified program- and system-level security gaps, and have evaluated, developed, and integrated multiple identity and access management solutions. They have implemented industry standard data encryption tools, and designed, developed, and delivered remote and on-site training and evaluation programs, as well as vulnerability and policy management and monitoring capabilities. With careful planning and implementation, organizations can protect and secure their information and network resources, anticipate and mitigate risks, and counter threats that impact mission-critical infrastructure and stakeholder value. [5] ■

References

1. WorldatWork—Staff Authors."WorldatWork 2008–2009 WorldatWork Salary Budget Survey: WorldatWork Survey Finds Telework on the Rise in the US, Canada." *http://www.worldatwork.org/waw/adimLink?id=28062* , August 2008
2. For more information on how to protect your organization from insider threats, see IATAC's State-of-the-Art Report (SOAR), *The Insider Threat to Information Systems.*
3. GTD Times Team—Staff Contributors. "What is GTD?" *http://www.gtdtimes.com/2010/02/22/what-is-gtd/,* February 2010
4. Bekele, Demi & Bates, Brian, J. "Meeting Security Perils of Telework and Alternative Work Arrangements." GSA Real Property 2009 Policysite Newsletter, July 2009
5. Ibid.

About the Author

Brian J. Bates, CISM, PMP | possesses 13+ years of progressive leadership in the fields of information assurance, cybersecurity, project and program management, performance measurement and monitoring, and secure telework. Brian possesses a MBA focused on Human Resources/Marketing Research, and a BA in Economics/Employment Relations. He received his PMP and CISM certifications in 2006 and 2009, respectively. Brian serves the leaders of higher education, commercial, and government by providing guidance and support to their respective projects and security performance measurement and monitoring programs. Brian has also presented at the ACSAC and RSA Security conferences in 2008 and 2009, respectively.

Letter to the Editor

Q *The last edition of the* **IAnewsletter** *had a one-page article on US Cyber Command. Since its inception, is the Cyberspace Integration Group (CIG) Charter still in effect?*

A As tasks for the National Military Strategy for Cyberspace Operations were closed out last year, the CIG came to an end. The purpose of the CIG was to monitor progress of the tasks under this plan to ensure they were aligned with similar efforts.

The CIG was comprised of senior military leaders across the services as well as the National Security Agency (NSA) and the Defense Information Systems Agency (DISA). It was established by the direction of the Joint Chiefs of Staff and the Secretary of Defense.

Though the CIG is not still relevant as an organization, there had been ongoing discussions at the Joint Staff, Strategic Command (USSTRATCOM), and USCYBERCOM levels to determine whether or not a follow-on group similar to CIG should be established. With USCYBERCOM's activation, the roles and functions of this group were also under discussion.

As USCYBERCOM changes the general makeup of the Combatant Commands collectively, it is likely that similar changes will take place in how senior national leaders address cyber security functions as a whole.

For more information about how USCYBERCOM will impact Combatant Commands and our national defense, we plan on publishing a follow-on article in our next edition of the *IAnewsletter* that discusses USCYBERCOM's impact on the warfighter. ■

Workplace Privacy in the Cyber Age: Really?

by Kevin L. McLaughlin

In conjunction with the integration of cyber technologies into the work and daily life of employees, organizations are experiencing larger than ever losses of data. Much of this critical data loss ends up being caused by trusted employees, temporary staff members, and affiliates that work inside of the organization. These breaches occur against electronic data with enough frequency that employers are forced to consider taking steps which could be considered an invasion of employee privacy rights. This article discusses the extent to which employers should be allowed to monitor employee actions in the workplace, as well as the amount of privacy an employee should expect in the workplace.

Legal, Regulations, Compliance, and Investigations

The Central Question

Some researchers note that electronic monitoring in the workplace has become as ubiquitous as electronic communications and argue that employees have come to expect it (if not accept it). Should employers be restricted in the scope of electronic monitoring of their employees? Does electronic monitoring in the workplace infringe on employees' rights to privacy?

Organizations continue to take large scale losses and even go out of business by making the mistake of not adequately protecting their business critical data assets. These critical data assets can be in paper or electronic form. In this article, they are defined as data assets which are critical to organizational success, or assets which need to be safeguarded in accordance with various regulatory requirements. Critical data which is required to be protected and cared for is being stolen from companies at an alarming rate: in 2008, there were 540 electronic and 116 paper breaches resulting in 35,691,255 records stolen. [1] These losses, many of which were due to internal theft and dishonesty by full time trusted employees, cost US businesses between $60 and $120 billion annually. [2]

Tools that provide organizations and employees ease of transporting and access to data make it so that, "employers need to concern themselves with the online activities of their employees." [3] These employees have more access, intentional and unintentional, to organizational data than they ever had in the past: "Since the very first IT survey on cyber-attacks, one fact has remained almost constant: a greater percentage of attacks come from the inside—60% to 70%—than from the outside." [4] Employers have seen the risk and impact of internal theft rise steadily, and this rise in risk is causing them to give serious thought to just how much monitoring of employee activities should take place in the workplace.

> Since the very first IT survey on cyber-attacks, one fact has remained almost constant: a greater percentage of attacks come from the inside—60% to 70%—than from the outside.

Information Security and the Workplace

"Data breaches, unfortunately, have become a way of life for corporate America;" [5] breaches are so frequent that the victims of them are almost becoming de-sensitized to the loss of their personal and private data. While attending a November 2009 Chief Information Officer (CIO) symposium, I overheard two CIOs talking. One of them said, "I am tired of hearing about Information Security. By now they (Information Security Professionals) should realize we get it." I had to bite my tongue. If other CIOs really "got it" we would be seeing a downward, not upward, trend in information breaches. Is it unfair to point the finger at CIOs? Maybe, but with 35 plus million pieces of electronic data stolen from organizations in 2008, the senior manager responsible for safeguarding critical data assets needs to

step up and take ownership and responsibility. The CIO, by title, and by design, is often the senior manager within an organization with responsibility for the organization's information and information assets. Organizations need to quit fooling themselves. In a 2010 SC Magazine survey titled "Guarding against a Data Breach," 91% of the respondents stated that they felt their organizations were "taking the right steps to prevent customer or other critical data from being stolen." [6] With breaches steadily rising, and only 54% of organizations having one to five Information Security specialists to help them come up with strategies to mitigate the risk of breaches, many of which are caused by trusted insiders, it is time for better self awareness on the part of the organization managers who are responsible for safeguarding the data. [7] The sheer numbers of breaches require organizations to consider different and possibly more aggressive approaches to breach prevention. Employee workplace monitoring and tracking is an example of aggressive breach prevention methodology.

In order to discuss workplace monitoring we must first define the workplace. Technology like the Blackberry has "further blurred the already fuzzy lines separating the workplace from the individual's personal world." [8] Employers like Procter & Gamble, a Fortune 35 company based in Cincinnati, Ohio, are internally marketing tag lines like "Work-Life Blending"—a concept that encourages employees to use technology tools in order to work when and where they choose to. Organizations and employees need to figure out where personal privacy and workplace privacy begin and end when an employee is blending their work life into their personal life.

Organizations and employees need to figure out where personal privacy and workplace privacy begin and end when an employee is blending their work life into their personal life.

Employer vs. Employee

Some employers feel that the potential legal liability associated with employee misuse of cyber equipment during the workday is such a great risk that they are contemplating forgoing monitoring of e-mail and Internet and simply removing all external e-mail and Internet access from the workplace. After all, don't they own the work and work time of the employee? [9] However, this legal liability risk must be weighed against the potential performance impact caused by the lowering of employee moral if such draconian steps are taken. Consider that salaried employees work until the work is complete and often stay at the workplace until so late in the afternoon that banks, stores, *etc.,* are closed. Having Internet accessibility actually facilitates them remaining onsite and working longer. With Base Realignment and Closures (BRAC) affecting thousands of Department of Defense and Government employees, the same basic thought premise on security and productivity can be applied to salaried telecommuting workers. Considering the potential negative effect that removal of basic items like e-mail and Internet access may cause to the overall workforce and employee morale, the better alternative may be to implement extensive and detailed usage monitoring instead:

> *A company shouldn't care whether employees spend one or 10 hours on the Internet as long as they are getting their jobs done…It is probably better that an employer stay away from the issue [of Internet usage]; otherwise, it might lose an incredibly productive employee. [10]*

How then does extensive workplace monitoring impact the employee's right to privacy? Ambiguity abounds in the topic area of workplace privacy. Who has more rights? The employer who needs to protect their assets, or the employees who feel that

US courts continue to rule that any potential disclosure eliminates the right to privacy, and as long as they do so, employer property rights will continue to trump employee privacy rights.

their privacy is protected under the Fourth Amendment right against unreasonable search and seizure? To answer these questions, the whole concept of privacy needs to be examined; both personal privacy and workplace privacy should be considered. Kang states that "privacy is a chameleon that shifts meaning depending on context." [11] Since as far back as 1987, courts have ruled on workplace privacy in cases like *O'Connor v. Ortega,* with rulings that seem to support Kang's chameleon analogy by making contrasting statements like, "government employees can have a reasonable expectation of privacy in the workplace," and, "the government employer or its agents can conduct searches and monitor for work-related reasons, even if they violate an employee's Fourth Amendment rights." [12] Rulings like this, while somewhat contradictory, are not unexpected as the leaning of the courts tends to be that the employer's common law personal property rights, with respect to electronic devices, will trump the employee's perceived right to privacy. [13] Further, electronic discovery cases like Zubalake, which imposed severe sanctions for intentional, negligent, or even accidental destruction of data, are pushing employers to employ sophisticated surveillance technologies to mitigate liability. This employment of surveillance technologies can be viewed as placing employee privacy in serious jeopardy. [14]

US courts continue to rule that any potential disclosure eliminates the right to privacy, and as long as they do so, employer property rights will continue to trump employee privacy rights. [15] Further, since the US Constitution really does not specify anything about the right to privacy—"constitutionally based privacy rights in the US have been the result of judicial interpretation of constitutional amendments" [16]—it is somewhat surprising that employees assume that they have a basic right to privacy in regards to employer monitoring. The Fourth Amendment clearly dictates that people have the right to be secure in their persons, houses, papers, and effects. The hinge point and key word is "their." During work hours and when using company owned assets, regardless of where these assets are located, a solid case can be made that the employee has no right of ownership to these assets or to the work area they are using; therefore, they are subject to whatever monitoring the organization—who is paying for their time, who owns the equipment, and who owns the workspace—puts in place. The exception to this monitoring is the right to be free from monitoring in areas that are deemed intimately personal, like restroom or locker room facilities. [17] Sprague in his article titled *Orwell Was an Optimist* states that:

> *As employees spend more time at the workplace, and spend more time working at home…the dichotomy of privacy protection between…home and the less protected workplace begins to break down. Employees, for the most part, are unable to bring the stronger home-based privacy protections into work while, at the same time, employer interests begin to intrude upon the perceived sanctity of the home. [18]*

Organizations have been placed in the driver's seat in regards to their ability to make decisions which impact workplace privacy as the courts "have largely looked to ownership of property and not the inviolate personality of employees when ruling on reasonable expectations of privacy." [19] Examples of this stance by the courts can be seen as far back as 1996 when a court ruled that there is no expectation of privacy in workplace e-mail. Subsequent rulings have definitely favored the employer's interest in the area of establishing expectations of privacy within their workplace and for their workforce. [20]

As long as the organization strictly follows its policy to exercise its prerogative to search employee offices, desks, workstations, and other electronic tools, it has the right to do so. [21] New advances in electronic monitoring are giving employers the capacity to monitor just about everything employees are doing, and the cost impact to the organization for implementation of these monitoring tools is minimal. Along with this monitoring comes the revelation of a "legal reality that is distasteful to many: that there is no independent right to privacy in the workplace." [22]

Conclusion

Monitoring of employees and their activities in the workplace is not a new thing. Employee monitoring has taken place since ancient times in the form of overseers, foremen, managers, *etc.* Foremen occupy critical positions because they manage, plan and define work, communicate with workers, and motivate them to perform and not slack off. Foremen also monitor and observe to make sure that employees are following safe work practices. [23] Employers, and for the most part US courts, have consistently held that while an employee is being paid to do a task for the organization, they may be monitored and observed for a multitude of reasons. This has been extrapolated to include that the equipment and workplace owned by an employer is not a private area for an employee.

According to the Clinton Administration's Information Infrastructure Task Force (IITF), privacy is "an individual's claim to control the terms under which personal information—

information identifiable to the individual—is acquired, disclosed, and used." [24] But this is just one of many conceptualized definitions of privacy, and because multiple definitions abound for privacy, we struggle to place proper individual privacy borders in the workplace. An individual privacy border is a three dimensional square box that surrounds each of us. This privacy border is where we put our inviolate items, and our expectation is that no one will enter or intrude upon this border without our explicit permission. It is critical to the creation of clear legal guidance for the courts to define which workplace items, if any, can be placed inside individual privacy borders. Once these inviolate items are defined, then employers would have full rights and authority to perform detailed monitoring and surveillance on all activities that are not part of individual privacy borders.

Lacking clear guidance from the judicial branch, employers are in a tough spot trying to figure out how much of an employee's privacy they should violate in order to better safeguard critical data assets. In the areas that lack legal precedent, organizations should create an internal policy that clearly dictates what they are going to monitor as well as areas in which the employee should not have an expectation of privacy. Policies are an efficient way to both clearly define workplace privacy boundaries and show employee understanding of the established boundaries. The clear effect of new policies that many organizations are putting in place is that they can and will monitor and search their computer networks for any and all purposes. [25] These policies should be supported by signs and screen banners that remind employees that during their working time they, along with the equipment they use, and the area they work in, are subject to electronic and physical monitoring.

Organization-owned and employee-used systems should be monitored in such a way as to ensure that the ability to commit insider theft is largely mitigated. It is necessary to have security awareness programs that explain: why organizational monitoring of systems is necessary, how the systems are going to be monitored, which systems are going to be monitored, and who is going to have access to the information gathered during monitoring. These same security awareness programs need to demonstrate the new office etiquette required of employees in the cyber workplace. Employees should understand that they need to do their part to use organization-owned equipment appropriately. [26] ■

About the Author

Kevin L. McLaughlin | began his career as a Special Agent for the Department of Army. He has had many careers over the years, including Police Officer in Kissimmee, FL, middle school teacher, Director at Kennedy Space, President of his own company, and IT Manager and Senior Information Security Manager with the Procter & Gamble (P&G) company. Kevin earned his MS in Computer Science from NOVA Southeastern University. He holds several certifications, including: CISM, CISSP, PMP, ITIL Master Certified, GIAC Security Leadership Certificate (GSLC), and is currently working on his PhD from the Student University of Fairfax. 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. Data Breaches Skyrocket in 2008. IDTheftResourceCenter. 2, Mar/Apr 2009, Information Management Journal, Vol. 43, p. 15.
2. Safeguarding Corporate Secrets. Swartz, Nikki. 5, Sep/Oct 2006, Information Management Journal, Vol. 40, pp. 24–30.
3. Workplace Privacy in the Cyber Age. Collier, Debbie. 2002, Industrial Law Journal (Juta), Vol. 23, pp. 1743–1759.
4. Securing Against Insider Attacks. Lynch, David M. 1, July 2006, EDPACS, Vol. 34, pp. 10–20.
5. Blind Sided. Brandel, Mary. 6, Feb 9, 2009, Computerworld, Vol. 43, pp. 27–31.
6. Minding Data. Armstrong, Illena. 1, January 2010, SC Magazine, Vol. 21, pp. 28–33.
7. Ibid.
8. Somebody's Watching Me: Workplace Privacy Interests, Technology Surveillance, and the Ninth Circuit's Misapplication of the Ortega Test in *Quon v. Arch Wireless*. Conforti, Justin. 461, 2009, Seton Hall Circuit Review, Vol. 5, pp. 461–496.
9. Workplace E-mail Privacy Concerns: Balancing the Personal Dignity of Employees with the Proprietary Interests of Employers. Isajiw, Peter J. 2002, Temple Environmental Law & Technology Journal, Vol. 20, pp. 73–104.
10. Inappropriate Internet Surfing. Verespej, Michael A. Feb 7, 2000, Industry Week, p. 58.
11. Information Privacy in Cyberspace Transactions. Kang, Jerry. 1193, 1998, Stanford Law Review, Vol. 50, pp. 1193–1294.
12. Expectation of Privacy? A Brief History, Including Long, Larson, and DoD's New Computer Use Policy. Dukes, Thomas. 3, 2007, The Reporter, Vol. 35, pp. 22–25.
13. Workplace Electronic Privacy Protections Abroad: The Whole Wide World is Watching. Herbert, William A. 3, 2008, University of Florida Journal of Law and Public Policy, Vol. 19, pp. 379–420.
14. New Office Etiquette. Petrini, Catherine and Thomas, Rebecca. October 1995, Training & Development, p. 14.
15. The Need for a Revitalized Common Law of the Workplace. Corbett, William R. 1, 2003, Brooklyn Law Review, Vol. 69, pp. 91–162.
16. Herbert, op. cit.
17. Kang, op. cit.
18. Orwell Was an Optimist: The Evolution of Privacy in the United States and Its De-evolution for American Employees. Sprague, Robert. 83, 2008, John Marshall Law Review, Vol. 42, pp. 83–134.
19. Isajiw, op. cit.
20. The Information Privacy Law Project. Neil, M. Richards. 1087, 2005, The Georgetown Law Journal, Vol. 94, pp. 1087–1140.
21. Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices. Schwartz, Paul M. 2000, Wisconsin Law Review, pp. 743–788.
22. Cyber-working or Cyber-shirking?: A First Principles Examination of Electronic Privacy in the Workplace. Kesan, Jay P. 2002, Florida Law Review, Vol. 54, pp. 290–332.
23. Privacy, Ideology, and Technology: A Response to Jeffrey Rosen. Cohen, Julie E. 2029, 2000–2001 Georgetown Law Journal, Vol. 89, pp. 2029–2046.
24. Kang, op. cit.
25. Dukes, op. cit.
26. Conceptualizing Privacy. Solove, Daniel J. 2000, California Law Review, Vol. 90, pp. 1087–1156.

Delivery Options for Upstream Intelligence

(Article 4 of 7)

by Tyson Macaulay and Chris Mac-Stoker

The Upstream Intelligence articles included in this edition are part of a seven article series. Readers can find more UI articles in the Summer 2010 edition and the upcoming Winter 2011 edition of the IAnewsletter*.*

This article seeks to explore core technical issues associated with the delivery of Upstream Intelligence (UI), as it was defined in the previous articles. In these articles we sought to establish a framework and taxonomy for UI and discuss possible business models which might allow current cyber-threat intelligence to evolve into full UI.

After deciding to employ UI associated with zero-day, malware compromises, the next two decisions are about: 1) the frequency with which the UI should be delivered/consumed, and 2) the appropriate manner in which the UI should be delivered/received/acted upon.

This article addresses the subtle but critical challenges associated with the distribution of UI from the aggregation and correlation engines, to the subscribers and end-users of this intelligence.

This article addresses the subtle but critical challenges associated with the distribution of Upstream Intelligence (UI) from the aggregation and correlation engines, to the subscribers and end-users of this intelligence.

Upstream Quality of Service

Quality of service (QoS) requirements are typically bound to the application under consideration: e-mail, voice, video, or industrial control systems for example. Each of these systems will require a certain threshold of confidentiality, integrity, and availability associated with the delivery of their data from source to destination before the service degrades beyond usability. Confidentiality requirements are related to the data confidentiality and intended audience, while issues related to integrity and availability are also "hard coded" into application requirements. Nonetheless, QoS requirements can differ substantially from application to application. Privacy is sometimes considered a fourth element of assurance; here we will consider privacy as an aggregated, business-level requirement re-stating properties of confidentiality, integrity, and availability.

UI is a service whose QoS requirements have not been widely considered, yet such a discussion is necessary to facilitate the design of delivery systems. Defining differing levels of QoS for UI enables cost flexibility and broader adoption among a wider range of potential subscribers, and substantial macro-level social and economic benefits associated with better mitigation of a growing range of cyber threats. QoS requirements for UI will in turn drive not only costs, but also impact the technical delivery choices.

Intelligence Interface

A challenge associated with UI is the structure of the "intelligence interface." An intelligence interface is the business and technical constructs that allow for sensitive information to be exchanged among distinct parties. These parties may be different organizations operating at a mutually agreed or equal level of assurance (they trust each other—or at least have been told to trust each other); alternately, the parties may be operating at different levels of assurance (at least one party does not fully trust the other). The intelligence interface defines not only how information may be exchanged technically, but what type of information is exchanged, on what frequency, and at what level of detail. [1]

These issues of who sees what intelligence also have precedents in the financial markets, where trading houses

deliberately resist the possibility of their positions being exposed to competitors. The cyber-threat intelligence intended for distribution through this work is highly sensitive and not necessarily appropriate to distribute as a simple block of data to all parties equally. For instance, if the cyber-threat intelligence reveals that a certain retailer is suspected of suffering a compromise, is it appropriate that other, subscribing retailers receive this intelligence? At the same time as the victim institution?

Types of Cyber-threat Intelligence

As discussed earlier in this series of articles, there are two fundamental variants of threat and therefore Upstream Intelligence: "threat-from" and "threat-to." Threat-from is about the threat agent, its resources and characteristics; in the context of cyber-threat this information is composed of things like IP address, DNS name, Autonomous System Number (ASN), port, and protocol. Threat-to intelligence is more asset-specific. Threat-to information is about either the indications (both obvious and subtle) of targeted and tuned attacks converging on a specific asset, or about suspicious communications outbound from an asset: an indicator of compromise (a successful attack).

Assurance Requirements of Upstream Intelligence

Threat-from and threat-to are distinct types of intelligence possessing distinct assurance requirements. It is important to understand this differentiation because the delivery options available to each assurance level can be different, and if the two types of intelligence are delivered together, then the delivery technology must be designed appropriately.

Assurance Property	Sensitivity	Description
Confidentiality	Moderate	In general, the confidentiality of threat-from information requires moderate levels of assurance. The confidentiality requirement associated with threat-from information derives largely from the commercial value of the information itself. In some instances, such as military applications of UI, threat-from information may be highly strategic in that the threat agents do not yet know they have been detected, therefore substantially elevating the confidentiality requirement.
Integrity	High	The integrity of threat-from information requires high assurance, since the accuracy of a UI threat list is a key differentiator from stand-alone, signature-based malware identification. The ability to corrupt a threat-from list would result in their ability to cover up compromises and remain undetected.
Availability	Moderate	Generally, the availability of threat-from information also requires moderate levels of assurance. Availability requirements are defined by the ability of the consuming party to process and manage the threat-from data. While threat-from information is highly dynamic, changing on a second-to-second basis, update-on-change is beyond the requirements of many potential subscribers who lack the resources to handle such an intelligence stream in real time. However, it is likely that certain public safety and military organizations will place a premium on availability and look specifically to consume UI as it is minted, in real time.

Table 1 Threat-from Assurance Requirements

Threat-from Assurance

For many subscribers to UI services, threat-from intelligence will have a lower assurance requirement than threat-to intelligence (see Table 1). Threat-from information is about malicious or compromised IP addresses on the internet and defines external sources (or destinations) which should be monitored with suspicion.

Threat-to Assurance (Table 2)

Threat-to intelligence concerns targeting or compromising information about assets owned by the subscribing entity (see Table 2). For this reason, to many subscribers to UI, threat-to intelligence will have higher assurance requirements than threat-from intelligence.

Assurance Property	Sensitivity	Description
Confidentiality	High	The confidentiality of threat-to information requires high levels of assurance. Threat-to information contains intelligence about assets currently under attack or compromised. Disclosure of this information represents enterprise-level risks associated with brand or reputation, competitive positioning, service-level breeches, and possibly regulatory compliance. As a result, threat-to information needs to be managed in a manner such that, as far as possible, only asset owners are entitled to threat information about their own assets. However, it is possible that threat-from information may result in the disclosure of a compromised device associated with an identifiable business (because that device had become a source of threat—not only a victim). [2]
Integrity	High	The integrity of threat-to information requires high assurance, since accurate threat-to intelligence represents previously unavailable, quantitative metrics about the force and velocity of targeting by threat agents. The ability for threat agents to corrupt a threat-to list would result in their ability to cover up their compromises and remain undetected.
Availability	High	The availability of threat-to information requires high levels of assurance. However, once threat-to information for a given entity changes because a compromise or attack has been observed, this information must be propagated as quickly as possible. Availability requirements are also defined by the ability of the consuming party to process and manage the threat-from data. As an Upstream Intelligence service-provider, the assumption must be made that subscribers are in a position to consume changes immediately as they become available; therefore distribution mechanisms should be designed to meet this requirement.

Table 2 Threat-to Assurance Requirements

	Sample Subscribers	Uses
Real-time/on-change	All entities with the ability to consume UI	Compromise detection, incident response, forensics
On-demand	Devices and organizations operating without dedicated internet links	Compromise detection, incident response, forensics
Periodic (daily/weekly)	Last resort solution for less sophisticated online entities, small business, consumer, Internet Service Provider	Compromise detection, incident response, forensics

Table 3 Threat-to Delivery QoS

	Sample Subscribers	Uses
Real-time/on-change	Military, critical infrastructure	Critical infrastructure protection, intelligence gathering, surveillance and interdiction
On-demand	Universities, laboratories, product vendors, devices and organizations operating without dedicated internet links	Perimeter security and wide area monitoring, research and development
Periodic (daily/weekly)	Law enforcement, online business, data center providers [3]	Perimeter security and wide area monitoring

Table 4 Threat-from Delivery QoS

Quality of Service in Upstream Intelligence

Threat-from and threat-to intelligence will have different QoS requirements, where threat-to intelligence about targeted assets will be rated higher for the simple reason that it may contain information about compromised devices and not just targeting information. Threat-to information about compromised devices should be readily distinguishable and contain alerts that act like a fire alarm indicating trouble on the internal side of your infrastructure. Threat-from information is about the general malicious intent in the world and is used to perform analytics with internal network elements, especially for organizations with multiple gateways to the internet. Threat-from intelligence is intended to support further analysis, and does not necessarily demand the same immediate sort of response that threat-to intelligence about a compromised device might warrant. As a result, threat-from intelligence will be handled in a less urgent manner and therefore have lower associated QoS—and possibly even distinct delivery mechanisms.

Tables 1 and 2 outline distinctions between the sensitivity of threat-from and threat-to UI. Table 3 and Table 4 are examples of how service levels might be defined to address this range.

Support Architectures for Service Levels

The mechanisms and designs discussed here are not immutable; in fact, it is most likely that these designs will be combined, augmented, and streamlined according to the needs of specific users and possibly never deployed entirely as described below.

Push-On Change / Real-time Designs

The following are high-level approaches to the challenge of delivering UI to subscribers in a manner that is both fast and secure. To the knowledge of the authors, these designs are viable today, but theoretical or at least not publicly operational.

Figure 1 is an on-change/real-time intelligence distribution system based largely on multicast [4]—a member of the Internet Protocol (IP) family increasingly available in large carrier networks, though

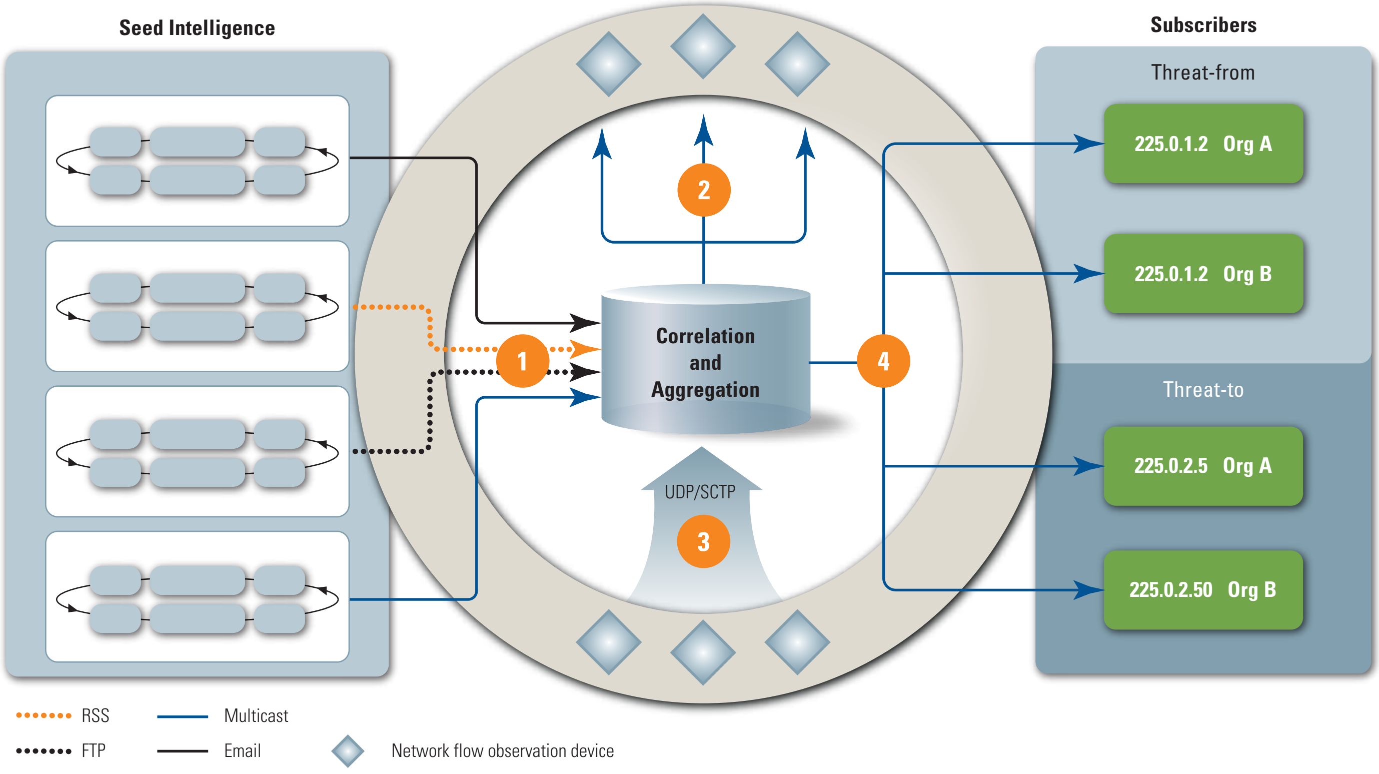


Figure 1 Multicast Upstream Intelligence Distribution

not supported on the internet. Multicast is an excellent delivery vehicle for UI because it is a very fast and light protocol for delivering small, rapidly changing information elements—such as IPs, ASNs, and domains. Multicast can also be deployed in a manner which makes it very difficult to attack. The source of multicast traffic can be obscured so that observation does not reveal the source, and therefore offers no attack vectors other than brute force denial of service on the entire (carrier) network. Similarly, the one-way communication properties of multicast make it possible to establish sources behind multiple, hardened layers of routers and firewalls with only pinhole egress allowed.

Feature "1" within Figure 1 shows the seed sources delivering intelligence about suspicious or bad IPs, ASNs, and domains through a variety of means. Ideally, they too would apply multicast for delivery, but the diversity required for good sourcing means a very flexible collection interface is necessary. After initial correlation and aggregation of seed sources, "2" shows these constantly changing lists propagating to network elements immediately on change using multicast to add, remove, and update the IPs, ASNs, and domains on the "watch list" at the carrier or service-provider border. Once instructed to observe and report traffic to and from anything on the watch-list, "3" shows an even larger body of intelligence flowing back to the aggregation engine as a "grey list" of devices now considered threatened or suspicious due to communications with watch-list devices. Now stream protocols such as User Datagram Protocol (UDP) or Stream Control Transport Protocol (SCTP) are used to accommodate a constant flow of information. [5] The devices actually generating the stream back to the aggregation engine could conceivably be software-defined routers, or intermediate devices that might be gathering netflow, filtering based on the watch-list, and re-transmitting the segments of interest. After receiving the grey list, the aggregation engine weighs and classifies the resulting UI grey list according to multiple different classes of QoS and threat-to/threat-from, "4" is the use of multicast to then deliver the different types of UI to subscriber groups, with the highest grade of QoS as near to real time as possible. Where "real time" means as soon as an IP engages in grey list activity, it is identified to subscribers.

Caveats

The amount of information that may require aggregation and correlation will be vast, and while some capabilities currently exist within vendor products, they may never have been deployed in this manner. Similarly, existing carrier and service provider infrastructure may not have the processing and storage capacity to support UI and enhanced netflow reporting without major upgrades.

As an alternate approach, Figure 2 illustrates a "packet staining" system that might be deployed by a carrier or service-provider with enhanced network elements. Under such a system, UI is collected and aggregated as per steps 1 to 3 in Figure 1. UI is then distributed back to network elements such as border and core routers with a multicast or similar real-time delivery capability. The elements then change certain ephemeral portions of the IP packets with sources or destinations matching those in the constantly updated UI watch-list. For instance, the *Differentiated Service* field, also

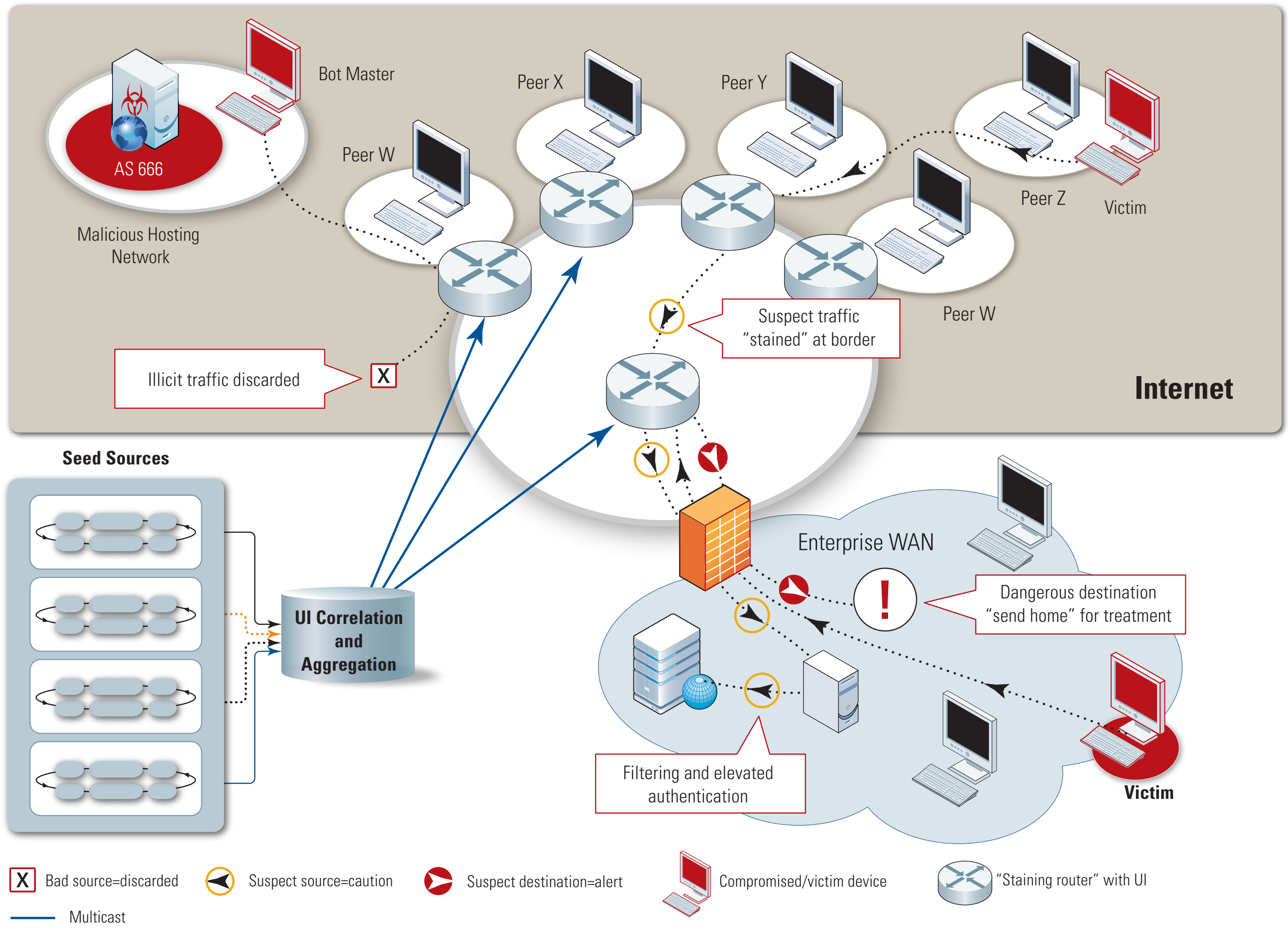

AS 666
Malicious Hosting Network
Bot Master
Peer W
Peer X
Peer Y
Peer Z
Victim
Peer W
Suspect traffic “stained” at border
Illicit traffic discarded
X
Internet
Seed Sources
UI Correlation and Aggregation
Enterprise WAN
!
Dangerous destination “send home” for treatment
Filtering and elevated authentication
Victim
X Bad source=discarded
Suspect source=caution
Suspect destination=alert
Compromised/victim device
“Staining router” with UI
Multicast

Figure 2 Packet Staining with Upstream Intelligence

known as type-of-service (ToS), within the IPv4 header is unused because ToS is not implemented on the internet. Alternately, the Options field within the IP packet could be altered to support UI flags without violating packet integrity. These changes amount to a “stain” on the packet which would be transparent to any device not looking for it, but would not alter the flow of the packets by routing through scrubbing or analysis centers—a tactic detectable by malware operators through induced latency and observable route-changes. Because the ToS field supports 6 bits of data, it could theoretically apply up to 64 different types of stain. As shown in Figure 2, packets from the worst sources within the UI information-base might be immediately directed to null interfaces and purged before entering the network. [6]

It would be a business decision as to whether to make staining a value-added or standard service. It may be the case that some subscribers want only the cheapest possible bandwidth and are satisfied with their ability to manage threats, in which case they decline to pay for staining. This being the case, staining may be applied according to both source (derived from UI) and destination IP, ASN, or domain of subscribing entities.

In either case, (ubiquitous or subscription-based staining) the perimeter devices of the subscribing entities may then apply their own policy according to the stain. The policy options may include decisions to elevate authentication, divert to analysis centers, or discard outright.

Another use-case related to staining applies to egress traffic from organizations: where traffic from these sources attempts to reach destinations within the UI watch-list, the network elements may choose to also stain these packets and re-direct them back to the organization through an IP tunnel on an alternate interface for incident response (as in Figure 2). [7]

“Push-on change” is a process in which no information is sent to subscribers until something changes, such as a new entry, an entry expires and is deleted, or a property changes: then only the incremental change is “pushed” to subscribers. Push-on-change can be implemented in many ways other than those described here. However, a singular strength of these two approaches is that they are very difficult to disrupt because they utilize networks and elements which frequently exist, but are largely inaccessible to internet-based threat agents. Multicast uses a class of address that is not routed on the open internet and therefore the interfaces are not usually accessible except to those specifically subscribing to the UI service. Similarly, existing network elements which might engage in staining are already very well hardened and their management interfaces are not available through the open internet. This inaccessibility, coupled with the real-time delivery capabilities of multi-cast, further improves overall system assurance. What is more, in the case of multicast it is possible to deploy it in such a manner that even the source of the information is non-specific (versus source specific multicast), [8] meaning that even in the event that the multicast network delivering the UI becomes visible to threat agents, they might not even be able to determine where to direct attacks.

Query-based, On-demand Designs

Query-based UI delivery systems represent the current state-of-the-art in malware and threat intelligence delivery. Query-based systems are available from anti-virus and intrusion detection system (IDS) vendors and services such as Spamhaus. [9] The anti-virus and IDS vendors maintain on-line repositories of the latest malware and attack signatures for their subscribers to download on demand or according to a schedule. Alternatively, Spamhaus uses a DNS-based system to distribute information about the reputation of e-mail senders; users query the Spamhaus DNS service with the domain of the sender organization, and Spamhaus replies with one of about 11 different replies. The Spamhaus replies indicate whether the sender is good or bad, and the possible degrees or causes of this determination.

Another existing on-demand system that could easily be deployed for UI distribution is the widely used Really Simple Syndication (RSS) framework and family of tools for news syndication and other "feeds." But there is literally no end of possibilities associated with the adoption of on-demand systems, right down to homemade cronjobs (scheduled scripts configured by administrators).

Query-based systems continue to develop and become more sophisticated, with some vendors looking to provide software development kits (SDK) to allow third-party elements and applications to access more sophisticated threat information such as proprietary watchlists.

However, these query-based systems have at least two weaknesses in comparison to the "push" systems discussed above: first, they do not propagate intelligence on change—thousands of new pieces of critical threat intelligence might change between queries; second, their delivery models currently depend on the internet and are therefore subject to attack.

Conclusion

Through a consideration of the variety of possible QoS requirements of UI, it becomes apparent that there is a wide range of user-types and assurance requirements. The current means of delivering malware and threat intelligence are probably insufficient to support the growing demand for proactive UI. Query-based systems are well understood, easily implemented and cost-effective; however, they are subject to attack and cannot entirely meet the future needs for real-time delivery of UI. To support real-time response to compromise in a threat environment where fractions of a second really count, multicast-based delivery systems are the next logical step. ■

References

1. See Tyler Akers, *Taking Joint Intell Operations to the next level,* Joint Force Quarterly, National Defense University, issue 47, 2007 and David Strachan-Morris, *The Future of Civil-Military Intelligence Co-operation Based on Lessons Learned in Iraq,* 2008.
2. This conflict between the need for high integrity threat-from and high confidentiality of threat-to requires discussion beyond the scope of this paper.
3. Law enforcement QoS is intended to recognize the current resourcing and associated ability to pursue and prosecute, not including "child safety" operations.
4. See IETF RFC 3740 Multicast Group Security Architecture—*http://www.ietf.org*
5. See *Introduction to Stream Control Transport Protocol—http://tools.ietf.org/html/rfc3286*
6. See IPV4—*http://en.wikipedia.org/wiki/IPv4* and Differentiated Services—*http://en.wikipedia.org/wiki/Differentiated_services*
7. See IP in IP—*http://en.wikipedia.org/wiki/IP_in_IP*
8. See *An Overview of Source Specific Multicast—http://tools.ietf.org/html/rfc3569*
9. *http://www.spamhaus.org/*

About the Authors

Tyson Macaulay | is a Security Liaison Officer for Bell Canada, with 18 years of Information and Communication Technologies (ICT) security experience. Tyson 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). Tyson'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 *www.tysonmacaulay.com.*

Chris "Skip" Mac-Stoker | is a Distinguished Engineer within NIKSUN Inc.'s Innovation Center. With two decades of experience in advanced IP, OS core, and hardware technologies, Mr. Mac-Stoker is focused on supercomputing, performance, and security and data integrity concerns for the financial industry & other large-scale infrastructure consumers.

The Air Force Institute of Technology—Center for Cyberspace Research

by Juan Lopez, Jr. and Dr. Richard A. Raines

The Center for Cyberspace Research (CCR) was established in March 2002. The center is located within the Department of Electrical and Computer Engineering at the Air Force Institute of Technology (AFIT) on Wright-Patterson Air Force Base in Dayton, OH. CCR anticipates and responds to the changing educational and research needs of the Air Force, the Department of Defense (DoD), and the federal government by conducting defense-focused research at the Masters and PhD levels. CCR faculty conduct research and develop advanced cyber-related technologies including network intrusion detection and avoidance, insider threat mitigation, cyberspace situational awareness, network visualization, software protection, anti-tamper technologies development, and Critical Infrastructure Protection.

On June 19, 2008, the Secretary and Chief of Staff of the Air Force designated AFIT and CCR as the Air Force's Cyberspace Technical Center of Excellence (CyTCoE). The CyTCoE promotes cyberspace education, training, research, and technology development and facilitates the development of Air Force education and training in support of cyber operations as well as identifying and providing subject matter experts that understand doctrine, techniques, and technology to ensure dominance and superiority in cyberspace.

The designation as the Air Force's Cyber Technical Center of Excellence enhances CCR's ability to be a clearinghouse for "who does what" and "who needs what" in cyber. In that role, the center develops and strengthens relationships with and awareness of the activities of various cyber-related research, education, and training communities within the Air Force, service partners in DoD, federal agencies, and civilian academic and commercial research organizations around the globe.

Educational Opportunities

AFIT offers two fully-accredited cyber degree programs at the Masters level: Cyber Operations and Cyber Warfare. In addition, traditional Masters and PhD programs in Computer Science, Computer Engineering, and Electrical Engineering provide the opportunities for cyber specialization. AFIT programs are open to US citizens and provide opportunities for non-military students who are seeking a Masters Degree in Cyber Operations through a grant from the National Science Foundation (NSF) Scholarship for Service Program (CyberCorp). In this program, students earn a cyber security-focused Masters in return for federal government service upon degree completion equal to the time of fellowship support.

To support the Air Force and DoD mission to grow its cyber security workforce, the Center has developed two cyber Professional Continuing Education courses, Cyber 200 and Cyber 300. These courses, three and two weeks in length respectively, are taught at the classified level, blending current cyber policy, doctrine, and legal with applications of emerging technologies by hands-on experimentation.

CCR Research and Faculty

Defense-focused research is a key mission of the Center. CCR faculty possess extensive operational experience in military communications and security. In addition, the faculty have close working relationships with DoD, Department of Homeland Security, and Air Force organizations. This synergism promotes an environment for collaborative research that solves real-world communications and security issues facing our nation and national defense. On-going research includes:

- Biometrics and radio frequency identification
- Cyber force development
- Digital forensics and software protection
- Insider threat mitigation strategies
- Intelligence amplification
- Intrusion detection, mitigation, and avoidance
- Network management and security
- Supervisory control and data acquisition systems
- Security architectures, systems modeling and policies
- Social networking and engineering
- Software protection
- Wireless network security
- Wireless communications exploitation and security

▷▷ continued on page 30

Dr. Barry E. Mullins & Lt Col Jeffrey W. Humphries, PhD

by Juan Lopez, Jr. and Dr. Richard A. Raines

The Air Force Institute of Technology (AFIT) Center for Cyberspace Research (CCR) is at the forefront of cyberspace education and research. Our faculty and staff push the envelope to maintain currency in cyberspace trends and are very engaged in discovering the emerging technologies of tomorrow that will keep the Air Force and DoD out front in network-centric warfare. The mixture of civilian and military faculty at AFIT provides depth and breadth in cyberspace research that is unparalleled at similar institutions. The following two CCR faculty members highlight a sample of the range of expertise and mentoring available for graduate students that engage in cyberspace research as part of their degree programs at AFIT.

Dr. Barry E. Mullins

Dr. Barry E. Mullins is an Associate Professor of Computer Engineering in the Department of Electrical and Computer Engineering at AFIT and a valued member of CCR. He received a BS in Computer Engineering (*cum laude*) from the University of Evansville in 1983, an MS in Computer Engineering from AFIT in 1987, and a PhD in Electrical Engineering from Virginia Polytechnic Institute and State University in 1997. Prior to joining AFIT, he served as a computer and electrical engineer in the Air Force for 21 years. He is a registered Professional Engineer in Colorado and a member of Eta Kappa Nu, Tau Beta Pi, Institute of Electrical and Electronic Engineers (IEEE) (senior member), and American Society of Engineering Education (ASEE). He has also earned six professional certifications in the information assurance and information security domains.

His students applaud his infectious enthusiasm for the course material and instruction. He teaches several courses at AFIT including Computer Systems Architecture, Computer Architecture, and Advanced Topics in Computer Networks, in addition to two new courses he developed called Introduction to Computer Networking and Cyber Attack. He created Cyber Attack to address the increasing need to provide educated leaders in the cyber domain an introduction to the use of cyber to attain national security objectives. The course reinforces classroom instruction with numerous hands-on exercises including a comprehensive “capture the flag” final exam.

Dr. Mullins’ research interests include cyber operations, computer/network security, computer communication networks, embedded (sensor) and wireless networking, and reconfigurable computing systems. His recent research has focused on hypervisor introspection, malware detection *via* a graphics processing unit, cyber attribution, polymorphic networking, novel deep packet inspection methods, quantifying wireless multimedia performance, and efficient key distribution techniques for mobile networks. During his time at AFIT, he has graduated 22 MS students and one PhD student, and has published over 90 scholarly articles, book chapters, journal articles and conference papers. His research students have excelled, winning several “best paper” and presentation awards as well as the CCR’s Cyberspace Research Excellence Award the past two years.

Dr. Mullins is the 2010 recipient of the Air Force’s Science and Engineering Educator of the Year award. He was selected by the student body as the AFIT Instructor of the Quarter in Winter 2008 and again in Winter 2009. He was also awarded the Dr. Leslie M. Norton Teaching Excellence Award in 2009 by the AFIT Student Association as well as the Eta Kappa Nu Electrical Engineering / Computer Engineering Outstanding Teaching Award in 2009. The AFIT Board of Visitors also awarded him the Professor Ezra Kotcher Award for curriculum development for 2008. Moreover, prior to joining AFIT, he taught in the Department of Electrical Engineering at the US Air Force Academy (USAFA) for a total of seven years. During his time at USAFA, he taught over 860 students in 18 distinct courses and won three major teaching awards including USAFA’s Outstanding Academy Educator.

Lt Col Jeffrey W. Humphries, PhD

Lt Col Humphries is an Assistant Professor with AFIT’s Department of Electrical and Computer Engineering. He received a Masters in Computer Science from the Georgia Institute of Technology in 1993, and a PhD in Computer Science from Texas A&M in 2001. Prior to coming to AFIT, he served as flight commander, 116th Mission Systems Flight, 116th Air Control Wing, Warner Robins Air

▷▷ continued on page 30

Upstream Intelligence in the World of Legal Compliance and Liability

(Article 5 of 7)

by David McMahon and Tyson Macaulay

There is reticence on the part of the legal community to address cyber security problems without precedence. Ironically, vague privacy reasons are often justification to do nothing. The legal debate simply is not keeping pace with technology and tradecraft. Consequently, there is a widening gap between the laws and realities of cybercrime. Engineers and operators are making ethical, legal, and privacy decisions about cyber-security capability development and operations, without the benefit of a mature legal context. There is also a dearth of useful legal commentary and research in the area of advanced persistent cyber threats (APT). That which is published frequently lacks the benefit of operational experience and can be hypothetical and technically vague. Dr. Jennifer Chandler offers some of the more thorough discussions, even suggesting that legal or regulatory action is necessary to force private and public providers of Internet services to better protect their customers from cyber attacks. She argues that Internet Service Providers (ISPs) could be held liable for their role in hosting partly or entirely an attack, and that ISPs could have a proactive role by monitoring their end-users' computers and quarantine any infected machines *before* they cause any harm. [1]

Privacy and Jurisprudence

The strength and limitations of Upstream Intelligence (UI) and security services is often driven by the privacy debate. The difficulty in gauging social values and expectations is that these issues are so vastly complex that the nuances are well beyond the grasp of laypeople.

The following sections address some salient legal and privacy considerations for a number of active and proactive UI and security measures.

Traffic Shaping and Net Neutrality

The way in which one approaches privacy significantly affects the level of malicious traffic that can be cleaned from the Internet and to what degree ISPs can combat advanced threats. In most cases, privacy enhances security. However, too much freedom and lack of security controls, in the name of privacy, actually backfires, and destroys privacy. The original "Net-neutrality" concept comes from Lawful Access discussions, and referred to the ability of an ISP to maintain the integrity of their network architecture without police inserting intercept devices.

The privacy definition of *network neutrality* is a principle that advocates no restrictions on the use of the Internet. This includes a prohibition on any form of security monitoring, cleaning, or traffic shaping. Purist net-neutrality proponents have stated that ISPs ought not to observe or suppress malicious traffic such as: child pornography, criminal botnets, piracy, hacking, extortion, Distributed Denial of Service (DDoS) attacks, cyberwarfare, phishing, spam, or toxic content like hate, thus mooting UI capabilities. Net-neutrality submissions to the court have *claimed* that telecom companies seek to impose a tiered service model in order to control the pipeline and thereby remove competition, create artificial scarcity, and oblige subscribers to buy their otherwise uncompetitive services. There have also been allegations that ISPs and governments would use deep packet inspection devices to read or manipulate private communications for financial gain. However, net-neutrality advocates have failed to prove these allegations, and all claims have been struck down by Canadian courts. [2]

Bret Swanson from the Wall Street Journal said that,

> *YouTube, MySpace and blogs are put at risk by net-neutrality. He argues that today's networks are not remotely prepared to handle what he calls the 'exaflood,' and that net-neutrality would prevent broadband networks from being built, which would limit available bandwidth and thus endanger innovation.*

Additionally, Bram Cohen, the creator of BitTorrent noted,

> *Poorly conceived legislation could make it difficult for Internet Service Providers to legally perform necessary and generally useful packet filtering such as combating denial of service attacks, filtering e-mail spam and preventing the spread of computer viruses... it is very difficult to actually create network neutrality laws which don't result in an absurdity like making it so that ISPs can't drop spam or stop...attacks.*

Black Lists

Black lists and grey lists, as discussed in previous papers in this series, can be created from the domain names or IP addresses of known threats that have been harvested/discovered through a number of means. Black and grey listings are like credit ratings. However, threat actors change addresses rapidly and black lists must be constantly updated minute-to-minute. The reliability of sources and veracity of the data contained in black and grey lists used as part of upstream security and intelligence is critical. Mistakes can either overlook malicious sites or unintentionally black list legitimate sites. Upstream security providers may prefer that an independent third party compile the lists and assume liabilities, as per child safety initiatives in Canada (*cybertips.ca*) and the UK. This arms-length (transparent) approach between black list creation and implementation eases much of the liability concerns associated with one single party policing the portions of the Internet under their management.

Domain Name Services

Domain Name Services (DNS) is a primary control plain for the Internet. Most folks, or organizations for that matter, do *not* appreciate how vital DNS is to their security and privacy. The proper checks and balances must be put in place to allow providers to protect DNS, detect and mitigate APT, and derive (resell) threat intelligence from DNS monitoring without privacy obstructions. Conversely, DNS activity should not be shaped for competitive business gains.

Dark Space Traffic Flow Analysis

Dark address space is the area of the Internet's routable address space that's currently unused, with no active servers or services. By monitoring all traffic to and from dark space, it is possible to gain insight into the latest techniques and attacks and to trace victims and control nodes of a botnet, for example. Upstream security services can use darknets to identify threats with confidence with little impacts on privacy.

Content Monitoring

A real-time audit of communications flows (*i.e.,* e-mail) and corporate Information and Communications Technology facilities is not only common practice but is considered a best practice and obligatory under certain compliance regimes. Organizations must maintain positive control over both their infrastructure and *info*structure. This necessarily includes active monitoring. Acceptable use policies need to be enforced at the same time reasonable allowances are made for personal communications. Since most modern cyber threats are based on a social-engineering or content-based threat, it is necessary to examine content. There must, however, be a balance between content examination for threat management and privacy. To a large extent, this debate has been settled in jurisprudence.

Upstream Liability

Distributed Denial of Service

Distributed Denial of Service (DDoS) protection is a value-added, upstream-security service from service providers that only they can provide owing to the nature DDoS itself. Questions are being asked about whether such capabilities are optional:

> *There appear to be a variety of measures that ISPs can take that would help to impede the propagation of bot software or throttle botnet activity on their networks. Some of these methods may constitute an unacceptable exchange of freedom and privacy. With respect to DDoS attacks, ISPs can enforce 'egress filtering;' which monitors IP packets sent from their subscribers. [A victim of a DDoS attack] may soon find it worthwhile to sue [the ISP]. [However,] the plaintiff is contributory negligent for failing to employ anti-DDoS services. [3]*

Strike back

A tactical option in warfare is to counter-attack. Counter-attack or "strike back" when dealing with cyber threats is sometimes a tempting alternative to purely defensive postures and is enabled by UI; yet strike-back strategies also possess potential liabilities.

The most effective strategy to combating advanced cyberthreats, is to target threat networks before they go active. This necessarily requires good intelligence and a willingness to conduct pre-emptive proactive strikes against the threat networks and actors. There seems to be some reluctance for Western authorities to conduct such operations in cyberspace, even where there is no compunction to launching military strikes in real space. Any pre-emptive proactive operations would necessarily involve major telecommunications carriers and their upstream services from a number of perspectives: strikes would transverse the carrier network and either be blocked by upstream security mechanisms or be permitted through. Most governments simply do not possess the independent capabilities.

Authorities will need to conduct careful target templating and weapon selection before launching a counter-attack. Strike back, if over-employed, can be manipulated to provoke a reaction and redirect it towards a new victim. There is also the risk of collateral damage. Attacks by authorities can also be construed as acts of war since most attacks originate from foreign soil. Notwithstanding, offensive (proactive) cyber operations against an APT is the most effective tactic. Failure to engage in offensive operations, when it is the best option, may also be negligent. This is akin to authorities not arresting dangerous, armed criminals, owing to a decision *not* to arm officers.

An example of strike back gone awry are predatoral bots. [4] Predatoral bots are described as "goodwill mobile code which, like viruses, travel over computer networks, replicate and multiply themselves." One paper shows that "Lotka-Volterra" equations can be used to model the interaction between predators and viruses similar to the natural world. A good example of a predator is the W32/Nachi worm, which has been rated by McAfee Security as a moderate security risk. It tries to delete another worm called the W32/Lovsan worm, and place the relevant Microsoft patches onto a computer system that it has invaded. The predatoral bot in this case actually caused as much trouble as the original threat, and was just as illegal.

Now consider Laws of Armed Conflict (LOAC):

> *Much analysis into the implications of information operations using computers and the topic of Computer Network Attack (CNA) has pointed toward the existing LOAC. In the event that a CNA against a state is initiated by or involves a non-state actor, particularly outside the context of war, then the LOAC would not apply. The interesting point about this conundrum is that it indirectly supports the notion of conducting computer network evade operations and active defense/network defense operations in order to make the determination of the source of an attack as being state or non-state. The second point is that not all computer attacks will happen in times of declared war. This is where International treaties such as the United Nations Charter can be of use. States must conduct themselves within these agreements to keep any legitimacy on the international stage. The UN Charter's Chapter VII Article 51 offers states some allowances to act in self-defense. [5]*

In determining the proactivity of netcentric warfare that uses carrier infrastructures as a weapons platform, the "fundamental principles of military necessity, unnecessary suffering, proportionality, and distinction (discrimination), will apply to targeting decisions." [6]

Disposal of Botnets and Rendition

Are ISPs obliged to handover control of a criminal robot network to authorities as part of upstream intelligence capabilities? What if the botnet possesses extra-national or extra-judicial foreign intelligence potential? If a botnet is being used to rob citizens, then police on some level should be made aware. However, the problem of detecting, isolating, and delivering botnets to authorities is resource intensive. In a fashion, ISPs would be doing a significant amount of police-work with neither the public budgets nor legal authorities. As is often the case, authorities would come to rely on these upstream capabilities more and more.

Mandates and Legislative Gaps

Measuring the success of legislation to reduce cyber risk is difficult. Consider pieces of public policy related to cyber security from the last decade. When placed on a timeline and correlated using a T-Test to network flow over the same time period, there appears to be no measurable effect on the actual bandwidth of malicious traffic across private and public sectors. [7] Contrast this with non-legislative, operational security initiatives implemented by private carriers and service-providers which have had immediate and profound effects on malicious traffic loads and measurable reduction in cyber risk. This is arguable evidence that policy and legislation are missing the mark.

Policy and law might allow a company to transfer liability risk to those writing the regulations and standards defining compliance. For instance, intercepting and handing off botnet control to law enforcement is a slippery slope. Clear conditions and policy need to be in place to permit this to occur as well as controls around using carrier infrastructures as signals intelligence platforms. The provider must be able, under the law, to report/hand-over both criminal and threat networks without fear of legal liability. Similarly and more prosaically, a provider must *not* be obliged or directed to engage in upstream security and intelligence operations without regard for larger operational reality and especially remuneration. Conversely, providers should be cautious of deliberately hunting down APT on behalf of authorities for payment by eradicated threat (a bounty). Some form of delegation and perhaps out-sourcing of national-level cyber threat detection, investigation, and mitigation to private sector providers must occur, but rules of engagement need to be much clearer.

There is ambiguity in mandates. Combating advanced cyber threats naturally involves crossing numerous public sector mandates and private sector interests. Take for example a well orchestrated broad-based cyber attack against North American financial institutions from an organized criminal enterprise operating from a foreign country with the duplicity of the state. Whose responsibility is it to investigate, interdict, disrupt, and prosecute the end threat agent? Remember that "Blocking is not stopping." The procedural considerations are mine-fields of policy issues and mandates: the presence of private citizen information, jurisdictional governance and interpretation of roles, identification of converged threat agents (*i.e.,* criminal, espionage, terrorist). Responsibility centers, legal authorities, real capabilities, and legislative mandates do not align to the problem.

Criminal Code and Citizens Arrest

There exist provisions within many criminal codes that permit self-defense and citizen's arrest. These laws also apply to cyberspace. Citizen's arrest is meant for situations when police cannot respond in time to a serious crime. In the case of a fast-flux botnet that is propagating across a provider's subscriber base, unless the police can detect, reverse-engineer, take down the control channels and neutralize up to a million machines in under two (2) minutes, is the provider within its rights to take unilateral action? What are the limits of this action and how do they conflict with national telecommunications regulation and law? Privacy laws? Safety and security regulations within interdependent critical infrastructures?

Mandamus Prerogative Writs

Mandamus prerogative writs have been used by the private sector to compel the government to fulfill their mandate and public service. [8] Such writs can possibly be used to force public authorities to stop a cyber attack. According to such writs, should the government not be able to fulfil its role in this regard, then the private citizen or organization can use whatever means necessary to act, with the same authorities vested in government. Jurisprudence supports the citizen's and infrastructure owner's right to self-defense using reasonable force, including lethal force. In other case law, citizens have taken it upon themselves to address urgent matters of public safety, and invoiced the local governments. Similar arguments hold for cyberspace and the provisioning of upstream security services outside of a public service.

Public Nuisance

A person or organization is guilty of a public nuisance whose property is employed (consciously or unconsciously) to create an unreasonable annoyance or inconvenience to neighbors or the public. [9] This can be applied to an organization who propagates malicious network traffic, or perhaps those that fail to manage it when it was within their means. Upstream security and intelligence services from service providers potentially allow organizations to transfer nuisance and ancillary risks to the providers.

Civil Action

In British Common Law, an Anton Piller warrant is a court order that can be applied to permit upstream security providers the right to search premises and seize evidence without prior warning. This prevents the destruction of incriminating evidence, particularly in cases of alleged cyber crime, and piracy. Typically, this order is only granted if there is an extremely strong *prima facie* case against the respondent. A provider can use this authority where large amounts of malicious traffic or attacks are emanating from the respondents' external network interface and either transiting the provider facilities or directed at the provider's infrastructure.

Conclusion

There still persists a great deal of legal ambiguity by design, as it pertains to the thorny issues of upstream security, intelligence, and cyber defense in general. Depending on the jurisdiction, the legal, privacy, and policy community can be cautious and hesitant to wade into the discussion on rapidly evolving upstream security capabilities.

Broadly, an exposure has been created due to a lack of clear interpretation of legislation and mandates in the context of cyber security. In some cases, policy centers (department, agencies, bureaus, *etc.*) are concerned about exceeding mandates at the expense of progress and needed solutions. These policy centers may ultimately risk falling short of achieving basic expectations, negatively impacting public trust. An inactive defense is a sin of indifference. ■

References

1. Jennifer Chandler, *Liability for Botnet attacks: using tort to improve cybersecurity,* Canadian Journal of Technology Law, March 2006.
2. Telecom Regulatory Policy CRTC 2009-657.
3. Ibid. Jennifer Chandler.
4. 'Predators: Good Will Mobile Codes Combat against Computer Viruses' by Toyoizumi & Kara, 2002, p.11).
5. *Evaluating Canada's Cyber Semantic Gap* by LCol Francis Castonguay.
6. United States Department of Defense, *Joint Targeting. JP 3-60*, 13 April 2007, Appendix E-1.
7. Combating Robot Networks and their Controllers, a study by Bell Canada, for the Public Safety Technical Program, 2010.
8. See *http://www.duhaime.org/LegalDictionary/M/Mandamus.aspx* or for a fuller discussion see, USA Administrative Procedure Act (APA) (P.L. 79-404) Sample Case: *http://www.cba.org/cba/cle/pdf/Bellissimo.pdf*
9. See *http://www.duhaime.org/LegalDictionary/N/Nuisance.aspx* or discussion in case law related to issues such as global warming. *http://www.inece.org/conference/7/vol2/33_ClimateChange.pdf*

About the Authors

David McMahon | has an honors degree in computer engineering from the Royal Military College of Canada, and has spent the last 25 years with the military, intelligence, and security community both in the public and private sectors. Mr. McMahon is a widely published author on the subject of the cyberthreat and proactive cyber defense. Mr. McMahon is currently the adviser for National Security programs in Bell Canada.

Tyson Macaulay | is the chief contributor to all Upstream Intelligence articles. His articles are featured in the 13-3 and 13-4 editions, and will be featured in the 14-1 edition of the *IAnewsletter*.

DoDTechipedia Happenings

by Albert Arnold III

The title of this edition of the *IAnewsletter* is “Privacy & Enhanced Information Security.” Depending on your perspective, this could cover a very broad range of topics. Are you involved with research and development and concerned about protecting information? Are you concerned about your personally identifiable information (PII)? Do you work with international partners involved with privacy? DoDTechipedia can provide information on all these topics and the opportunity to collaborate with others for the most up-to-date thoughts and ideas.

There are many new postings added to DoDTechipedia every day. As of September 20, 2010, a simple search on “privacy” revealed 294 items.

- Do you need to know about Homeland Security Presidential Directive 12 (HSPD-12) and about the implementation of the Personal Identity Verification (PIV) across the federal government? It’s here. Use DoDTechipedia to reach out to your colleagues to find out how this impacts information sharing and privacy across the federal government.
- Do you need to file a complaint? You can find out about the Internet Crime Complaint Center (IC3) on DoDTechipedia. If you want to know if others are having similar issues, post a comment.
- Did you know that Defense Advanced Research Projects Agency (DARPA) recently released privacy guidelines for research and development? You can get to them from DoDTechipedia. If you have questions about the guidelines, pose them to the community.
- Are you having trouble remembering those 15 character passwords that need to be changed too often? DoDTechipedia has a blog with some useful ideas to help manage passwords.

DoDTechipedia is not just an information resource. It’s a traditional wiki. You can share knowledge, create blogs, and collaborate across “borders” with ease. As a reader of the *IAnewsletter*, you have a significant wealth of knowledge that could be beneficial to others. No doubt, you’re also working on cutting edge projects that may benefit from the knowledge of others. Be part of an online “discussion” with your fellow colleagues to develop solutions faster.

Getting started is easy. Just register with DTIC at *https://register.dtic.mil/wobin/WebObjects/DTICreg*. Your registration also allows you access to other DTIC products and services.

Go to *https://www.DoDTechipedia.mil* to begin using this collaboration resource. ■

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. Nominations are due 3 January 2011. For more information, visit *http://iac.dtic.mil/iatac.*

International Conference on Information Warfare and Security

by Carrie Solberg and Juan Lopez, Jr.

The Air Force Institute of Technology's (AFIT) Center for Cyberspace Research (CCR) proudly hosted the International Conference on Information Warfare and Security (ICIW) on April 8–9, 2010. This year's conference was held at the Hope Hotel and Conference Center at Wright-Patterson Air Force Base, marking the ICIW's fifth anniversary. Over 100 researchers from the United States, Estonia, Finland, France, India, Portugal, South Africa, Turkey, and the United Kingdom attended.

The conference chair, Dr. Michael Grimaila from CCR, explained that, "The ICIW conference provides a unique venue where researchers can discuss advancements of scientific and technical knowledge as it pertains to information warfare and cyberspace." This year we were fortunate to have two excellent keynote speakers: Dr. Michael VanPutte from the Defense Advanced Research Projects Agency (DARPA), who discussed mission assurance, and Dr. Steve Rogers from the Air Force Research Laboratory (AFRL) Sensors Directorate, who spoke about integrating humans and computers to address "wicked problems." The keynote speeches resonated well and generated many discussions about the complexity of operating in cyberspace.

ICIW goals include putting research into practice and giving researchers an understanding of real-world problems, needs, and aspirations. "The ICIW brought the 'who's who' of information warfare together at one location so that we could collaborate and discuss different ideas and research that everyone is doing. So as we walk away, we have a better understanding of what the community is doing and how we can solve problems for our nation," explained Dr. VanPutte.

You can find further information about ICIW 2010 and the keynote presentation at *http://academic-conferences.org/iciw/iciw2010/iciw10-home.htm*

CCR continues to be an advocate for cyber education and research. Hosting conferences is one approach to bring together researchers and practitioners from the cyber community to exchange knowledge concerning scientific and technical topics. CCR will host the 2011 Colloquium for Information Systems Security Education (CISSE) Conference June 12–15, 2011.

For further information about the Center for Cyberspace Research, visit the CCR home page at *http://www.afit.edu/ccr.* ■

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.*

▷ continued from page 22

The center currently includes seven core faculty members, 15 collaborating faculty members, five research associates, and 26 Masters and PhD student researchers. Since 2002, the center has produced over 250 publications and received over $25 million in research and infrastructure grants.

The Center for Cyberspace Research continues to evolve to meet DoD demands for cyber focused research and education and continues to develop partnerships with organizations to transition this research to the warfighter. Faculty, staff researchers, and students make presentations at various national and international conferences and symposia and most recently hosted the 5th International Conference on Information Warfare in Dayton, OH. For further information, please visit the CCR home page at *http://www.afit.edu/ccr.* ■

About the Authors

Master Sergeant Juan Lopez, Jr., CISSP, USMC (ret) | is a research engineer at AFIT. He conducts cybersecurity research in supervisory control and data acquisition systems, radio frequency identification, and wireless sensor networks. He received a BS degree from the University of Maryland, a MS degree from Capitol College, and a MS degree from AFIT under the Information Assurance Scholarship Program. He is currently pursuing a PhD in computer science at AFIT.

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

▷ continued from page 23

Force Base, GA. He oversaw direct support to wing-level cross-specialty functions to analyze, document, coordinate, validate, and track all Joint Surveillance Target Attack Radar System (JSTARS) software requirements. He directed active duty, Air National Guard and civilian personnel to evolve the JSTARS warfighting capability through an $18M/yr software process.

Lt Col Humphries' specialization lies in cryptographic analysis. He has been instrumental in the expansion and development of new cryptographic courseware and innovative research efforts. He has developed and teaches several courses including Secure Software Engineering, Cryptography, and Cryptanalysis. He is also the lead curriculum developer for the new Cyber Professional Continuing Education sequence, which every new cyber officer in the Air Force must complete. Lt Col Humphries ensures that what is learned in the classroom flows into DoD relevant research. He recently developed a one-of-a-kind Cybersecurity network test bed that will support real-world network operations. In addition, he is the principal investigator for CCR in support of an Air Force Critical Infrastructure Protection initiative to assess base security vulnerabilities. In this capacity, he is developing a cyber-assessment methodology to analyze and mitigate potential vulnerabilities in the critical areas of power, fuels management, and environmental controls. Finally, as a CCR representative to the President's National Security Telecommunications Advisory Committee, he helped draft the Report to the President on Commercial Satellite Communication Mission Assurance, identifying cyber security threats facing the commercial satellite industry and developed mitigation measures to combat such threats to national security.

His recent research has focused on public-key infrastructures, critical infrastructure protection, network trust management, and zero-knowledge proofs. During his time at AFIT, he has served as research advisor for eight MS students and has published numerous scholarly articles in various publications. He has also been an invited speaker at several different university forums. He was recently awarded the 2010 Excellence in Teaching Award by the Southwestern Ohio Council for Higher Education. In addition, he was named the 2009 Outstanding Military Faculty of the Year for the Department of Electrical and Computer Engineering. ■

FREE Products

Order Form

Instructions: All IATAC LIMITED DISTRIBUTION reports are distributed through DTIC. If you are not a registered DTIC user, you must do so prior to ordering any IATAC products (unless you are DoD or Government personnel). To register online: *http://www.dtic.mil/dtic/registration*. The *IAnewsletter* is UNLIMITED DISTRIBUTION and may be requested directly from IATAC.

Name ____

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
□ Computer Forensics (soft copy only. DTIC user code must be supplied before these reports will be shipped)
□ 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)

State-of-the-Art Reports (SOARs)

□ Measuring Cyber Security and Information Assurance
□ The Insider Threat to Information Systems (DTIC user code must be supplied before these reports will be shipped)
□ Software Security Assurance
□ A Comprehensive Review of Common Needs and Capability Gaps
□ 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)
□ 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 11	□ No. 1	□ No. 2	□ No. 3	□ No. 4
Volumes 12	□ No. 1	□ No. 2	□ No. 3	□ No. 4
Volumes 13	□ No. 1	□ No. 2	□ No. 3	□ No. 4

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

Calendar

November

USSTRATCOM Space Symposium
2–3 November 2010
Omaha, NE
http://www.afcea.org/events/

Cyber Security Readiness for the Federal Government 2010
3–5 November 2010
Arlington, VA
http://www.CyberSecurityReadiness.com

NSA Ops 1
16 November 2010
Fort Meade, MD
http://fbcinc.com/event.aspx?eventid=Q6UJ9A00LY86

NSA Ops 2
17 November 2010
Fort Meade, MD
http://fbcinc.com/event.aspx?eventid=Q6UJ9A00LY8X

NSA Ops R&E
18 November 2010
Fort Meade, MD
http://fbcinc.com/event.aspx?eventid=Q6UJ9A00LY94

December

Annual Computer Security Application Conference (ACSAC)
6–10 December 2010
Austin, TX
http://www.acsac.org/

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

SchmooCon
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

The 2011 Information Assurance Symposium
7–10 March 2011
Nashville, TN
http://www.informationassuranceexpo.com/

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

IATAC

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