# IAnewsletter

The Newsletter for Information Assurance Technology Professionals

Volume 5 Number 2 • Summer 2002

# Trust In Cyberspace?

also inside—

- GIG Interconnection Approval Process (GIAP)
- An Overview of the Evolving Law Related to Computer Network Defense
- Information Security Incident Response, Part II

# contents

## feature



## IA initiatives



## in every issue




About IATAC & the *IAnewsletter*—

*IAnewsletter* is published quarterly by the Information Assurance Technology Analysis Center (IATAC). IATAC is a DoD sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC), Defense Information Systems Agency (DISA).

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

Robert J. Lamb
Director, IATAC
703/289-5454

*IAnewsletter* Staff—

| | |
|---|---|
| Editor: | Robert J. Lamb |
| Creative Director: | Christina P. McNemar |
| Art Director: | Ahnie Senft |
| Designer: | Maria Candelaria |
| Analyst: | Abraham T. Usher |
| Inquiry Services: | Peggy O'Connor |

*IAnewsletter* Article Submissions

To submit your articles, notices, programs, or ideas for future issues, please visit http://iac.dtic.mil/iatac/news_events/author_submission.htm and download an "Author's 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
3190 Fairview Park Drive
Falls Church, VA 22042

Phone: 703/289-5454
Fax: 703/289-5467

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

Deadlines for future Issues—

| | |
|---|---|
| Fall 2002 | 23 August |
| Winter 2002/2003 | 25 November |

Cover design: Maria Candelaria
Newsletter design: Ahnie Senft

Distribution Statement A:

Approved for public release; distribution is unlimited.

# IATAC Chat

Robert J. Lamb, IATAC Director

*During the past year, we've had a number of organizations express interest in and receive training modules across a wide range of IA related topics. I thought it would be useful to summarize those courses here. While each has a core subject, they are easily tailored to specific requirements of a requesting activity.*

**Introduction to Information Assurance** provides a high level understanding of IA terminology, concepts, and technologies. Topics included are the different information states and the functions of confidentiality, integrity, non-repudiation, authentication, and availability. Additionally, this course provides an introduction to various IA technologies to include virtual private networks, firewalls, intrusion detection systems, smart cards, magnetic cards, and biometrics. (Course Length: ½ day)

**Risk Management** introduces the process of risk management, including risk assessment and mitigation within the context of information security. The course is designed to provide a thorough understanding of risk and the components of risk, an introduction to various methods of risk assessment including the Yellow Book's risk index formula, and an overview of automated risk assessment tools. (Course Length: ½ day)

**Computer Forensics** introduces the domain and defines forensic sciences and computer forensics in particular. It reviews the state of computer forensic science within law enforcement, addresses international implications, and offers techniques for performing forensic examination of computer media. In addition, the course presents concepts applicable to examinations of other media and operating system (OS) types. The course also includes hands-on training with COTS and GOTS tools used to support computer forensic examination. (Course Length: 1 day)

**Public Key Infrastructure** introduces PKI as it applies to a Defense-in-Depth strategy. The course is designed to provide an introduction to cryptography and security functions, PKI architectural framework, policy, public key enabled applications, and future trends. It provides a better understanding of PKI and how it can be applied within an organization. (Course Length: 1 day)

**Penetration Testing** provides an accurate depiction of the role of penetration testing in analyzing a system's overall security posture. The course provides a thorough understanding of penetration testing concepts, terminology, approaches, and techniques that can be applied to system and network configurations. This course is not intended to teach specific system vulnerabilities or how to exploit them, but will provide information on publicly available sources that are commonly used by hackers. During this course, attendees will learn how penetration testing fits into lifecycle system/network security and how it can compliment other commonly performed security activities such as risk analysis and security test and evaluation. (Course Length: 1½ days)

The **Law of Cyberspace** provides an understanding of the evolving legal framework in the domain of cyberspace. The course addresses both the substantive law (what is prohibited) and the procedural law (what legal processes must be complied with in investigating and prosecuting cybercrime, cyberespionage, or information war). It addresses international law and domestic law along with the legal complexities involved in transborder investigations. The domestic law portion highlights key statutory provisions including the implications of the USA PATRIOT Act of 2001. The course also explains the sometimes conflicting case law that has developed in interpreting laws in this field, with particular emphasis on legal traps for the unwary. The lessons of significant recent cases are examined, including the Gorshkov case (FBI obtained evidence by remotely accessing the subject's site in Russia), the Tennenbaum case (Israeli mentor in the Solar Sunrise case), the Skylarov case (defining the scope of the Digital Millennium Copyright Act), and others. At the completion of this course, attendees will have a better appreciation and understanding of the law of cyberspace, its requirements, pitfalls, and current trends in the law. While the course is taught at the advanced level, a legal background is not required as all legal terms and concepts will be fully defined and explained. (Course Length: 1 day)

A short version of this course was recently presented at SANSFIRE entitled "Do Borders Matter in Cyber Crime? Legal Issues Related to the Investigation and Prosecution of Trans-Border Cyber Crimes." Feedback from attendees was overwhelmingly positive. One attendee described it as "extremely invaluable for all security managers, engineers and legal professionals." Another attendee described it as "one of the best presentations I have heard this year. Make it a keynote presentation!"

All of the IATAC courses are available through either a subscription account or a technical area task. Information on obtaining these services are available on our Web site at http://iac.dtic.mil/iatac/news_events/training.htm. If you have any questions, please contact us at 703/289-5454 or iatac@dtic.mil. ■


By Dr. J. Bret Michael, Daniel R. Hestad, C. Martin Pedersen, and Leonard T. Gaines

# Incorporating the Human Element of Trust Into Information Systems Policy

## Exploring discretionary and mandatory policy about trust in terms of the structure and mission of an organization.

Trust is an inherently subjective notion. As such, trust is difficult to define, convey, measure, or specify. The individualistic nature of trust makes it difficult to incorporate into policy that can be applied across an organization. Yet trust policies within an organization permeate doctrine and procedures. Unfortunately, within those policies, trust is rarely defined; it is implicitly stated and individually interpreted.

To incorporate trust into doctrine or policy, one must first be able to define trust in the context of the doctrine, determine how and to what it is to be applied, identify why trust is important within the context, determine who will determine trustworthiness, and determine a measurement for success. In this article, we introduce a model that incorporates trust at the level of policy.

### Computational Models of Trust

Trust between humans is a cognitive function. Computational models of trust emulate and predict the way a human assesses trust. Existent models of trust that have been reported in literature represent attempts to assign metrics to trust-based relationships between humans and their computer-based proxies (e.g., intelligent agents). These models address the notion of trust in many different ways and their definitions and metrics vary significantly. Many different meanings and connotations of the term "trust" have been proposed. In fact, if one examines the many definitions, one might come to the conclusion that existing trust models are an amalgamation of different beliefs and ideas.

Developing models of trust for human interaction is difficult; it is even more challenging when dealing with information systems. People are much more comfortable evaluating trust that involves interpersonal interaction, because it is easier to apply personal experiences, perceptions, and personal observation. Trust involving information systems, especially in a distributed system, requires a different set of trust variables. More trust has to be placed in elements that are unknown to the user. Adding to the complexity is the fact that interpretations of trust can differ among computing bases, domains, and applications.

### Demand For Trusted Systems

The effective use of information technology and success in any organization requires trust, not only of the information communicated, but also among faceless communicators. Our belief in the validity of the complex and subtle messages we receive by telephone or electronic mail is conditioned on how well we know and trust the senders. In a sense, psychological bandwidth varies directly with the degree of trust between people. Trust cannot be decreed. The willingness to trust is a combination of values and evaluation, attitudes, and interests. National culture influences how and whom we trust. But within and across cultures, trust depends on whom we consider trustworthy and how well we create trust in others. [1]

Why are trustworthy distributed systems difficult to develop? Part of the problem is transitive trust. Transitive trust is where person A trusts person B. Person B trusts person C. However, that does not mean that person A trusts person C. In distributed systems, one entity does not have control over all of the various parts that make up the whole. The developer will never have direct control over the server operating system, router software or hardware, transmission medium, or database software that support the application schema. As a result, the user has to rely upon someone else to ensure that the various pieces are trustworthy. This problem is compounded when the distributed system pulls information from sources that are outside of the control of the developer.

### Trust and Distributed Information Systems

When an organization uses to some extent distributed information systems to support its decision-making processes, members of that organization should try to answer the following question: *How much trust can we place in these systems as face-to-face transactions become increasingly rare?*

Trust can be thought of in terms of faith or confidence. If a ladder looks wobbly, one is unlikely to trust it to hold one's weight. Now consider trusting the mechanisms for enforcing security policy on the Internet. If the Internet


mechanisms for enforcing authentication, authorization, privacy, integrity, and non-repudiation policy do not appear to be sufficiently strong to the users, then users may hesitate to use the Internet for conducting business. Trust can be lacking for reasons both real and perceived. One of the reasons there is not a high level of trust in the Internet for conducting business is that people simply do not understand the enabling technology or how to correctly apply it.

There are many ways of describing trust, as indicated by the results of literature surveys conducted by Hansen and Gaines. [2,3] For example Jøsang defines two types of trust; trust in humans and trust in systems. In terms of information security, trust in a system is the belief that it will resist malicious attack. Trust in a human is defined as the belief that the individual will behave according to a given policy or expectation, and will not act maliciously. [4, 5]

Trust in an individual computer can be established by a number of methods. The protocols used can be tested for compliance, the hardware components can be checked, and it can be measured against a trusted computing base (TCB). Trust can also be established by a set of evaluation criteria such as the Trusted Computer Security Evaluation Criteria (TCSEC), Information Technology Security Evaluation Criteria (ITSEC), and the Common Criteria. However, when dealing with a heterogeneous distributed computing environment such as the Internet, establishing trust is more difficult. The Internet has no trusted computing base. It is also not possible to test the trustworthiness of all of the hardware and software that, for example, a mobile agent might interact within such a system. As a result, some feel that the definition of trust is based on the belief that trust should only be placed in people, as they are the ultimate decision makers [6].

There are almost as many models of trust as there are definitions. Most of the models are similar in that they attempt to assign weighing factors to subjective variables. Jøsang developed a belief model and related calculus called subjective logic that assigns degrees of belief, disbelief, and uncertainty to opinions and utilizes logical operators to apply them to trust chains. [7] Most models are also similar in that they model trust from the perspective of a single individual. In this article we introduce a model of trust from an organizational perspective.

Neither a purely mandatory policy, nor a completely discretionary policy are sufficient in developing an operational model when one's organization is competing in today's highly competitive information domain. A hybrid, or synergistic policy that takes the most applicable qualities of both and applies them to an organization is required.

## The Discretionary-Mandatory (D–M) Model

The principles of the Discretionary-Mandatory (D–M) model [8, 9] for trust are defined as follows: Enable those at the lowest levels the freedom of making decisions based on their own unique situations; this is the discretionary aspect. At the same time, allow for direction and guidance from the upper levels of an organization in the form of mandatory policies, as well as a common set of rules and standards, which reflect the nature of the organization itself.

The D–M model is a synergistic organizational model which recognizes the value of over-arching management policies while at the same time understanding the need for distributed decision-making. The real value in the model is that it allows top-down, bottom-up, and lateral flow of information and trust while allowing decisions to be made at the lowest levels possible.

Mandatory policies are those rules and requirements written by either the central oversight or by a peer organization. Mandatory policies should be general in scope so as to not overly restrict the flexibility and adaptability of the organization. No policy can be written which covers all possible situations (see Figure 1 on page 6).

In this model, the system will enforce mandatory policies: it is not left to the user to decide which policies are discretionary and which are mandatory. Much like the system of state and federal laws in the United States, some laws apply to the entire country and some to individual states. It is not the citizen who decides which laws are relevant.

The need for mandatory policies is clear. In any organization, of any size, there should be a common set of goals and a common vision for where the organization is going. To further illustrate the need for a common mandatory policy, we have provided a simple diagram (see Figure 2 on page 7) to visually show the reader the importance of a common mandatory policy within one's own organization, or across multiple organizations. In our illustration, we use language as our example, where all nodes in a system must have a common understanding when policies overlap so all units can communicate. Mandatory policies are traditionally set in place by the senior leadership. The simplest explanation of this is to relate it to organizational behavior. One would not want the lowest level in an organization making decisions without guidance and leadership (see Figure 2 on page 7).

Allowing subordinate levels in an organization to develop their own methods of conducting their business, within an overarching framework, provides the flexibility and adaptability essential in the Information Age. The speed at which information is transmitted and processed requires senior leadership to forego total control and allow subcomponents of their company, even to the lowest levels, the ability and trust to make decisions.

Particularly in a large organization, such as the U.S. Department of Defense (DoD), one would not want to apply the exact same policy regarding trust on a geographic combat-

ant commander as you would the Naval Postgraduate School (NPS). The DoD is a complex organization, with many moving parts, each with multiple and diverse missions. Constricting each subcomponent into one set of policies is not the best strategy in today's fast-paced environments.

To further demonstrate the practical application of the D–M model, we have put together several examples to illustrate our D–M model. Our first example references urinalysis screening as applied to the U.S. Navy and its zero tolerance policy.

## Example: Zero Tolerance

The U.S. Navy has a zero tolerance policy for narcotics use. To detect violations, random urinalysis screening is conducted at each command. When a service member tests positive for illegal drugs, his case is sent to a review board to determine the legalities of the situation. The matter becomes somewhat subjective rather than objective due to differing legal interpretations of the scientific process of drug screening. So instead of having a true zero tolerance policy, the U.S. Navy allows each command some discretion depending on the extenuating circumstances of each case. The D–M model reinforces trust by providing guidance and standardization in the form of mandatory policies, but realizes the importance of flexibility in distributed decision-making on a case-by-case basis.

## Example: Software Maintenance

Consider the following scenario—

*The Program Manager of an information system at NAS Anywhere contracts with a local software development company XYZ to add functionality to the information system. XYZ accepts the contract, but does not have the in-house expertise, so they subcontract with company ABC in a third world country. ABC has an employee with anti-military views and inserts malicious code into the software, which subsequently deletes important files.*

This is a situation where a mandatory policy should have over ruled a discretionary policy. If the government's mandatory policy that software maintenance cannot be performed by third world nationals had been adhered to, the information system would not have been compromised. The program manager would still have the discretion to contract with XYZ, so long as they did not subcontract to foreign workers.

## Example: Aircraft Carrier Battle Group

A Carrier Battle Group (CVBG) is able to conduct sustained operations while being spread out over thousands of miles. The communications connectivity via satellite links for voice and data as well as point-to-point communications offers multiple paths across which data may be transmitted; this allows tactical and operational commanders to have access to constantly updated information about time-sensitive situations.

On the other hand, it also affords an adversary multiple opportunities to present deceptive information to our vast array of sensors in order to create confusion or give us a false sense of security. The goal of the adversary here is to extend the observe-orient-decide-act (OODA) loop so as to obtain a tactical advantage over the CVBG.

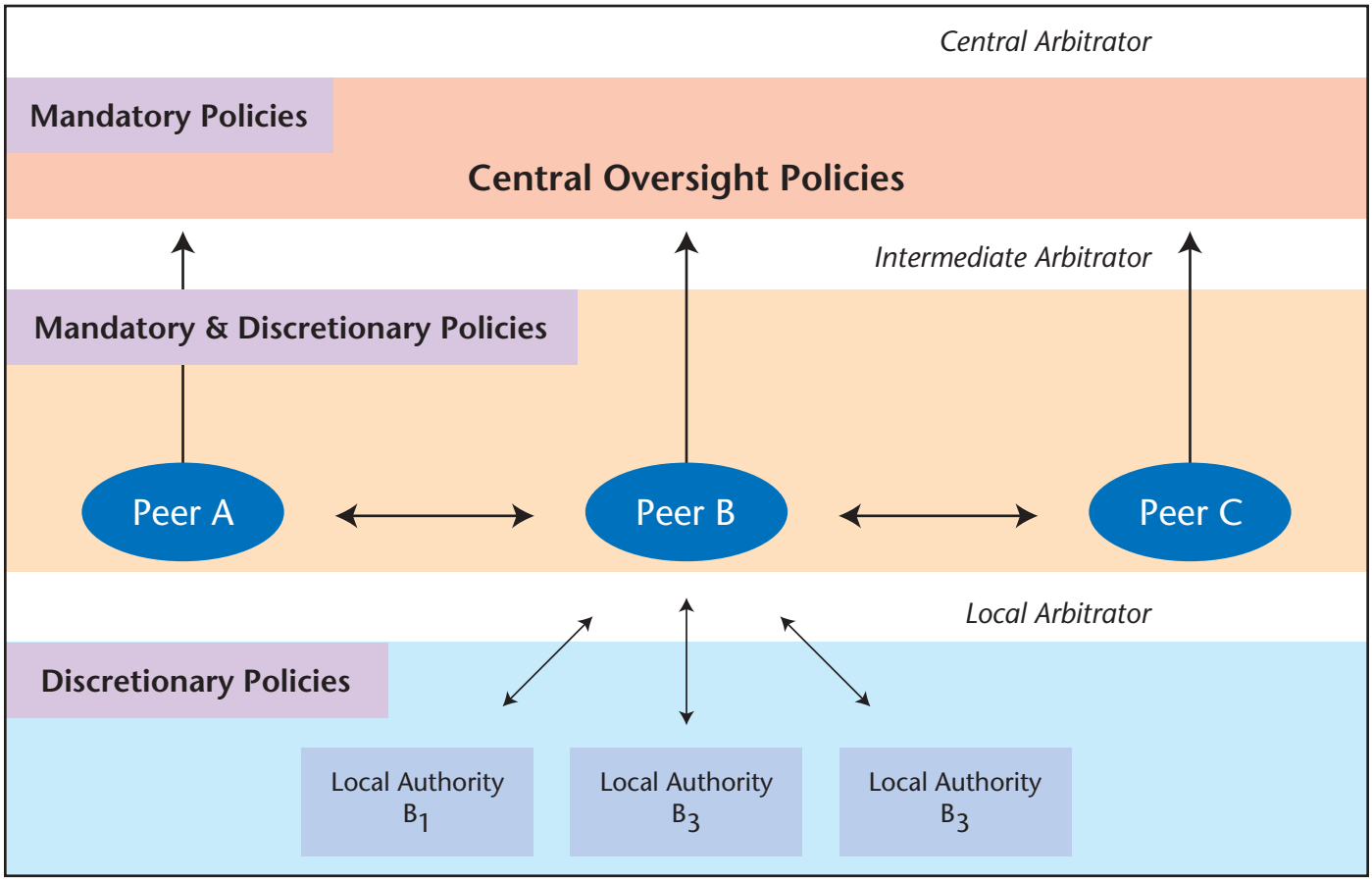



**Figure 1. Discretionary-Mandatory Model**

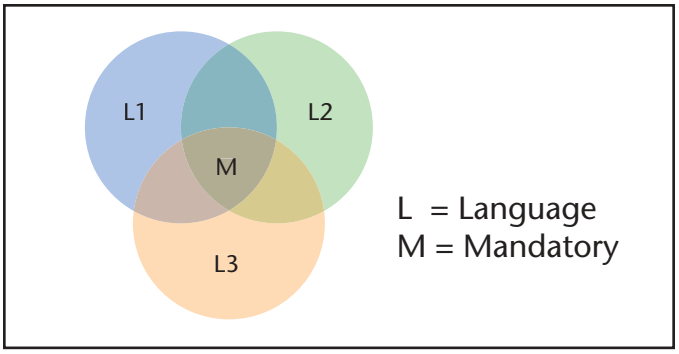



**Figure 2. Common Mandatory Policy**

When sensors acquire a contact, that information is transmitted to other platforms via a data link. It is also entered into a database to track over the long term. When the data on the contact is received by another platform, it appears on that platform's display in whatever symbology entered by the initial operator and classified by the contact's type (i.e., air, surface, or subsurface) as well as its relationship (i.e., friendly, unfriendly, or neutral). It is assumed that the contact was acquired, classified, and retransmitted correctly.

But this is not always the case. At each point, mistakes can be made. The contact could be a decoy designed to fool our sensors. The sensor operator could be newly trained and prone to error. In addition, the adversary, with the necessary transmitters and authentication procedures, could have inserted the data into the information system.

Moreover, it is not just an issue of receiving information and placing trust in that information, but also an issue of with whom are you willing to share that information. When the information is received from other organizations, issues of transitive trust must be addressed.

Consider the following scenario—

*A U.S. aircraft carrier is steaming in the Persian Gulf conducting normal flight operations. It has in company a U.S. Aegis cruiser along with an allied destroyer from nation X and an allied frigate from nation Y.*

*The allied frigate acquires radar contact on an unknown aircraft traveling inbound, which it classifies as hostile and transmits the track of the aircraft to the rest of the battle group. The frigate then loses radar contact with the aircraft but continues to update it as hostile in the shared database of the battle group.*

*The aircraft is then acquired by the Aegis cruiser at a distance of one hundred kilometers from the aircraft carrier. The Aegis system determines it is the same unidentified contact classified as hostile by the frigate. It is within the air-launched-weapons envelope of multiple theater threat aircraft.*

What should the Aegis cruiser do?

Although the U.S. Navy's doctrine and the standing rules of engagement would likely permit the Aegis cruiser to destroy the unknown aircraft, that would make little difference politically if the aircraft was a passenger jet. Alternatively, if the aircraft were hostile, then the Tactical Action Officer (TAO) would be held accountable for not engaging the aircraft.

The answer lies in how much the TAO trusts the information from the frigate. If there is an established relationship over time, common procedures, and training to establish trust amongst the two platforms, then the TAO can act with confidence on the information provided. However, if there are no commonalities, or established trust relationships, then the trust assigned to the information will be lower. The TAO also needs to evaluate his trust in his combat team, his own sensors, and the combat systems information systems.

If the cruiser's radars are confirming the same information as the frigate, then the TAO's trust in the information the frigate and his own systems are providing are going to be much greater. If the cruiser's radars provide conflicting information, the TAO's trust in the frigates information will be far less. The TAO may need to gather data from the destroyer before trusting the frigate's information.

Properly applied, the D–M model would account for the possible communication pitfalls in this scenario. Organizationally, the model would allow communication and procedural training to develop across platforms with no interference from a central authority, what we term "discretionary policies." This process would foster a more trusted relationship amongst the platforms. The model would also force the information systems to standardize their data integrity procedures by means of central oversight policies, which we term "mandatory policies."

The central oversight actor would be the operational commander, in this example the numbered fleet commander. He would promulgate mandatory policies to govern the actions of units in the operational theater. The peers would be the various tactical units involved in the operations: the aircraft carrier, the Aegis cruiser, the allied destroyer and the allied frigate. Local authorities would be the TAOs onboard the various units.

The fundamental concepts of the D–M model apply nicely to a dynamic, fast-paced and information-centric environment such as the battlefield. The model realizes the value of the input from the lowest levels; those who are directly involved in a situation and have the greatest need for accurate and precise information. At the same time, the model also allows for guidance, coordination and standardization from higher echelons in the organization. It also provides mechanisms for lateral communication inside an organization as well as communication across different organizations.

The D–M model is not reliant on a single input or piece of data and thus is insulated from single points of failure. It is easily applied to the short-term, single case decision-making situations. More importantly it applies to the long-term, strategic practices such as development of a Theatre Engagement Policy (TEP), foreign policy, economic policy; all of which, in their essence rely heavily on secure and trusted communications among many different countries, agencies, corporations, and people.

## Conclusion

There is always some degree of unpredictability associated with an information system due to misuse, lack of training, even general naiveté of the user. To construct systems with hard and fast mandatory security policies fails to recognize the human factors.

However, purely discretionary policy about trust is not the answer either. Such policy lacks the broad standardization to coordinate and share information outside the local domain. The answer appears to lie in an organized system that combines both discretionary and mandatory policies

to enforce agreed upon trust policy globally while permitting the human operators to use their discretion to evaluate the content of the information being shared at the local level.

There is ongoing research at the Naval Postgraduate School to further refine the D–M model. For instance, as part of his thesis research in the distance learning program in Software Engineering, Mr. George Walt of the Space and Naval Warfare Systems Center, San Diego, is exploring how to translate trust policy represented in the D–M model into system capabilities and requirements.

In addition, there is an ongoing collaboration between researchers at the Naval Postgraduate School and George Mason University to explore the technical feasibility of an approach for achieving adaptive system interoperability. In this approach, each local information system, within a system-of-systems, has a set of automated tools—known as a policy workbench—to aid in both the formulation and management of local policy. Returning to CVBG example, if the information-sharing policy for the shipboard command and control systems of nation X or Y changes, then the policy workbenches resident in the command and control systems of the Aegis cruiser could be used to query the policy interfaces of the systems of nations X and Y for such changes, reason about the changes, and update the local policy of the cruiser to maintain interoperability or some other property of the system-of-systems, including trustworthiness. ■

## References


1. Maccoby, M., Building trust is an art, *Research-Technology Management, 40*, 5, pp. 56–57, Oct. 1997.
2. Hansen, A. P., *Public key infrastructure (PKI) interoperability: A security services approach to support transfer of trust*, Master's thesis, Naval Postgraduate School, Monterey, CA, 1999.
3. Gaines, L. T., *Trust and its ramifications for the DoD public key infrastructure (PKI)*, Master's thesis, Naval Postgraduate School, Monterey, CA, 2000.
4. Jøsang, A., Trust-based decision making for electronic transactions, in *Proceedings of the Fourth Nordic Workshop on Secure IT Systems,* Stockholm University (Stockholm, Nov. 1999).
5. Jøsang, A., A subjective metric of authentication, in *Proceedings of the Fifth European Symposium on Research in Computer Security*, Springer-Verlag (Louvain-la-Neuve, Belgium, Sept. 1998), pp. 329–344.
6. Khare, R. and Rifkin, A. Weaving a web of trust. California Institute of Technology, 30 Nov. 1997; http://www.cs.caltech.edu/~adam/local/trust.html.
7. Jøsang, A. An algebra for assessing trust in certification chains, in *Proceedings of the Network and Distributed Systems Security Symposium,* The Internet Society (San Diego, CA, Feb. 1999).
8. Pedersen, C. M., *Trust and its ramifications for the DoD public key infrastructure*, Master's thesis, Naval Postgraduate School, Monterey, CA, 2001.
9. Hestad, D. R., *A discretionary-mandatory model as applied to network-centric warfare and information operations*, Master's thesis, Naval Postgraduate School, Monterey, CA, 2001.


## About the Authors


**Dr. J. Bret Michael**

Dr. Michael has been an Associate Professor of Computer Science at the Naval Postgraduate School since 1998. His research on information assurance and information operations covers many aspects of distributed computing. Dr. Michael is a member of the IATAC Steering Committee. He may be reached at bmichael@nps.navy.mil.

**LT Daniel R. Hestad, U.S. Navy**

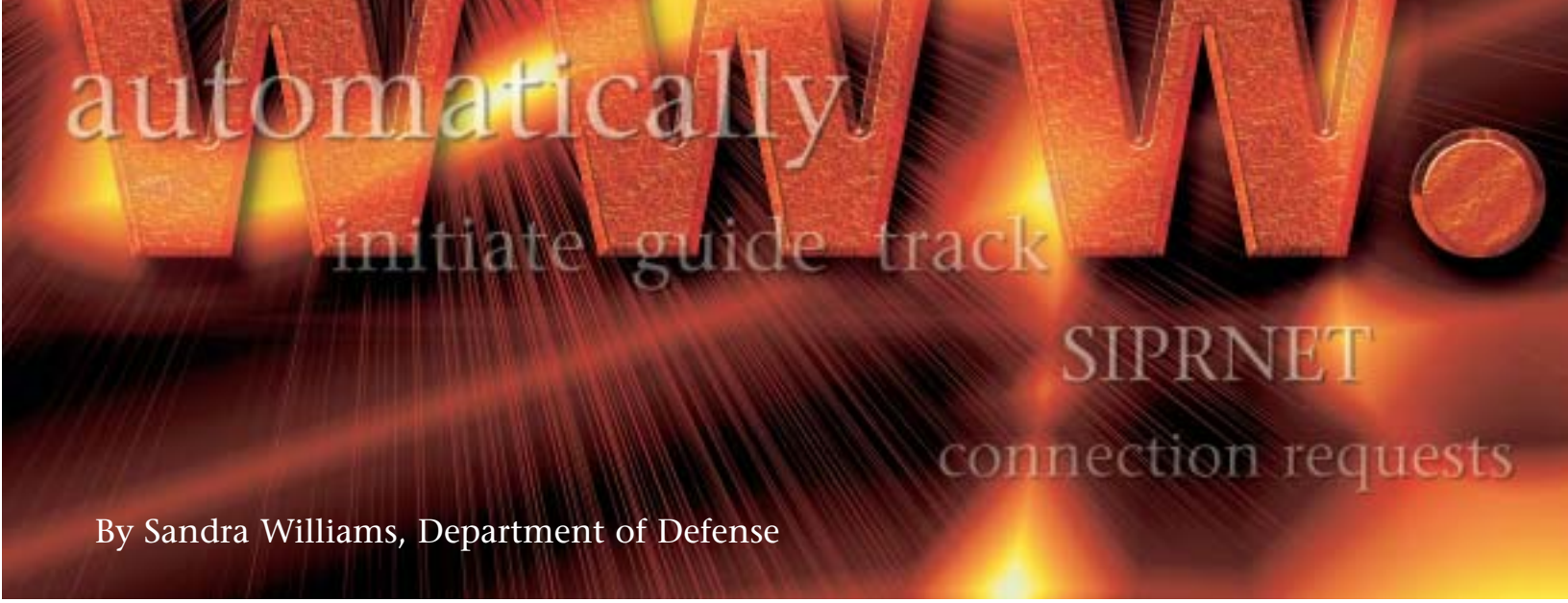
LT Hestad is a recent graduate of the Naval Postgraduate School's program in Information Systems and Operations. LT Hestad may be reached at drhestad@empire.eclipse.ncsc.mil.

**LT C. Martin Pedersen, U.S. Navy**

LT Pedersen is a recent graduate of the Naval Postgraduate School's program in Information Systems and Operations. He is currently with the U.S. Space Command, Colorado Springs, Colorado. LT Pedersen may be reached at martin.pedersen@peterson.af.mil.

**LCDR Leonard T. Gaines, U.S. Navy**

LCDR Gaines is a candidate in the doctoral program in Software Engineering at the Naval Postgraduate School. He is a graduate of the School's programs in both Computer Science and Information Technology Management. He is currently with the technical integration branch of the Naval Supply System Command, Mechanicsburg, Pennsylvania. LCDR Gaines may be reached at Leonard_T_Gaines@navsup.navy.mil.




By Sandra Williams, Department of Defense

# GIG Interconnection Approval Process (GIAP)




The GIAP is a new process directed by the four Defense Information System Network (DISN) Designated Approving Authorities (DAAs) (Directors of DIA, DISA, Joint Staff (JS), and NSA). The GIAP's purpose is to improve the security of the DISN long-haul backbone and connected enclaves by refining the processes involved in evaluating the various devices that connect and interconnect the three general networks that comprise DISN (NIPRNET, SIPRNET, and JWICS). You may ask, why would they create yet another process when there are already so many laborious, conflicting, time-consuming and expensive processes? Many customers who have a connection requirement encounter confusing processes and don't even know which process they are supposed to use.

Well, we have seen the problems and heard your complaints. We found that the processes are not broken, just independent, and they need to be synchronized. The GIAP was created with this in mind. It simplifies and consolidates the various connection approval processes into one easy-to-use portal that leads you directly to the process you need. Instead of receiving conflicting stories of your connection approval ticket status, there is a sole repository for all information pertaining to these tickets—the GIAP. And you, as the ticket-holder, can access your opened ticket to track it—you can see the timeline and status for yourself. Because the information contained in the database, when aggregated, is a snapshot of our tactical networks, we placed the Web portal on the SIPRNET (http://giap.disa.smil.mil). The following explains the GIAP in greater detail.

The GIAP is a Web-based one-stop shop created to automatically initiate, guide, and track SIPRNET connection requests. The SIPRNET Connection Approval Office (SCAO) at DISA manages the GIAP and submits connection requests to the appropriate approval process. This office is the single entry point for all your requests. The Web site utilizes simple "key questions" with yes/no answers that minimize mistakes that could lengthen the process. For example, a single security level request for SIPRNET connectivity will be directed to the SIPRNET Connection Approval Process (SIPRCAP). Requests for bridges between the SIPRNET and the NIPRNET will be routed through the Secret and Below Interoperability (SABI) process. Instead of separate databases for each process, which has created redundancy, the GIAP has a shared Oracle database that minimizes data duplication. The process was designed to be smooth and quick, and will make future connections consistent with Department of Defense (DoD) policy.

The SABI process is an important part of the GIAP. It is an Assistant Secretary of Defense for Command, Control, Communications, and Intelligence [ASD(C3I)] mandated process that establishes a uniform approach when connecting secret and below systems. It ensures interoperability for the warfighter within the level of risk accepted by the entire community with which it interconnects. Central to the SABI vision is protecting the integrity of and reducing the risk to the Global Information Grid by conducting vulnerability and risk assessments of each SABI connection. It implements the DoD Information Technology Security Certification and Accreditation Process (DITSCAP), a process mandated by the DoD. If you ever need to connect a secret system to a system of any classification level below it, you will go through the SABI process. And the GIAP will lead you there.

But we didn't just leave it at that. The GIAP Web site has incorporated education, training, and awareness (ET&A). You need to bridge systems of different security levels? Well, on the site you can find the SABI Referenced Implementation (SRI) which lists proven solutions that may meet your requirements—without creating a new system from scratch. This is the easiest and fastest way to get

*...continued on page 21*

By Rick Aldrich

# An Overview of the Evolving Law Related to Computer Network Defense



The law related to Computer Network Defense (CND) is a complex web of statutes and court decisions. Unfortunately, that web consists of gaping holes, conflicting case law, overlapping statutes, and the recognition of distinctions which technology has long since made obsolete. This is not totally unexpected. The traditionally slow evolutionary process of legal change has had difficulty keeping up with the extremely fast pace of changes in technology and the paradigm-shifting developments in CND. Nevertheless, significant progress is being made and the following discussion sets out a basic conceptual framework for understanding the legal landscape in this area.

Currently the law recognizes four fairly distinct roles, or "lanes of the road," in the area of CND. First, and perhaps most important to CND, is the service provider role. Representative players of this role are the Defense Information Systems Agency (DISA), the service Computer Emergency Response Teams (CERTs), and each network's Designated Approval Authority (DAA) and system administrators. Attacks against a network are most likely to be identified first by these service providers. Fortunately, Congress created a service provider exception to the general prohibition against interceptions set out in the Federal Wiretap Act (for more information see 18 U.S.C. §2511(2)(a)(i)). For law enforcement or counterintelligence agents to intercept such communications would generally require, in the absence of an exception to the Wiretap Act, a Title III court order or a FISA (Foreign Intelligence Surveillance Act) court order, respectively. Obtaining court orders can be a trying and time-consuming operation, so the importance of the service provider exception in providing a first warning of attack cannot be overstated. Service providers may also be able to rely on the consent exception, where users are required to sign user agreements or click through consent banners. Pass-through consent banners may establish implied consent. The consent and service provider exceptions are two separate and distinct exceptions and should not be merged into one as some want to do.

The second major lane in the road is that of law enforcement. It is important to note that computer intrusions can initially look very similar, whether they are in fact an information warfare attack from a foreign power, the work of a foreign intelligence agency, a terrorist attack, a criminal act, or the work of a "script kiddie." [1] Understandably, the law provides for radically different permissible responses in each case. Presidential Decision Directive 63, DoD policy, and the vagaries of the law have indicated the most appropriate means of resolving the identity and intent of the intruder, beyond that permitted to service providers, is through the use of law enforcement agents. Representative players in this role are the Federal Bureau of Investigation (FBI), the U.S. Attorneys Offices, and the Defense Criminal Investigative Organizations (DCIOs) [i.e., Air Force Office of Special Investigations (AFOSI), Naval Criminal Investigative Service (NCIS), Criminal Investigative Division (CID), Defense Criminal Investigative Service (DCIS)]. Some of these players have split personalities and can assume other roles as well, most commonly a counterintelligence role. This creates additional legal problems in the sharing of data even within such an agency. Some of those problems were resolved in the USA PATRIOT Act, which permitted increased sharing of information between law enforcement and intelligence entities. The overriding limitation to activities in the law enforcement area is the Fourth Amendment to the Constitution. Thus, law enforcement agents must generally obtain court authorization whenever their activities would contravene one's reasonable expectation of privacy. In fact, however, it is additional statutory layers of protection that Congress has added over the years that have caused the most difficulty. Up until the passage of the PATRIOT Act, law enforcement agents could not even attempt to identify a hacker, who had illegally penetrated a Government computer, without the hacker's consent or a court order. Some Government entities placed consent banners on their six or eight most commonly used ports in an attempt to obtain implied consent from trespassers. Unfortunately, since computers generally have over 65,000 ports, hackers were inevitably able to penetrate a system through an unbannered port and thereby bind the hands of law enforcement. The PATRIOT Act recognized a new exception for intercepting the communications of "computer trespassers." [2] Thus, law enforcement agents may now generally rely on the consent exception, the computer trespasser exception, or court orders to obtain the information necessary to accomplish their investigations.

There remain many other legal hurdles for law enforcement to negotiate in computer intrusion investigations domestically, and the law becomes much more complicated once one goes beyond the U.S. "cyber shoreline." International law and foreign country law will oftentimes require the use of letters rogatory or other time consuming legal processes. The new Convention on Cybercrime


attempts to facilitate international cooperation in the fight against cybercrime and makes some positive steps in that direction. Thirty-three countries, including the United States, signed it in December of last year, but only one country has ratified it so far.

The third major lane in the road is that of the intelligence community. Representative players in this role are the FBI, the Central Intelligence Agency (CIA), and the myriad of DoD intelligence components, including most notably the NSA and the Service intelligence components. What many do not seem to realize is that the intelligence components are also limited in their activities by the Fourth Amendment (at least as to activities within the United States or against "United States persons," as that term is defined in Executive Order 12333). Frequently the basis for an investigation within this lane comes initially from information provided by a service provider or law enforcement agent, working within their respective lanes, though some positive intelligence agencies operate specifically to gain advance intelligence of proposed intrusions. Intelligence agents will generally rely on consent, the computer trespasser exception and FISA warrants to obtain the information necessary for their investigations.

The last lane is the one for the warfighter. This lane is the least defined under the law. Certainly the President, as Commander-in-Chief of the Armed Forces, wields significant potential authority under the Constitution. Nevertheless the exact contours of that authority are unclear. President Truman's attempt to seize the steel mills during the Korean War was rebuffed by Congress and the Supreme Court in *Youngstown Sheet & Tube Company v. Sawyer*, 343 U.S. 579 (1952). Nevertheless, the reliance by the Court on Congressional action aimed specifically at narrowing presidential authority in that specific instance means the opinion leaves as an open question the scope of presidential power in the absence of such. Again, however, domestic law is only part of the equation. In the warfighting arena, the impact of the U.N. Charter and international treaties is also significant. Articles 51 (defining the scope of self-defense), 2(4) (defining what is an unlawful use of force), and Chapter VII (setting out permissible activities of the Security Council) of the U.N. Charter all figure prominently in the debate over what is and is not permissible. Whether such provisions even apply to "information warfare" is itself an unsettled question, though most would hold it does. Most legal commentators would also agree that the set of international law collectively referred to as the law of armed conflict also applies to information warfare, though this is also unclear since most of this law far predates computers and so one must apply new interpretations to established terms.

It is important to recognize that some governmental organizations may have subordinate entities playing in each of the four lanes. As such, it would make no sense to ask whether the government or even, for example the U.S. Air Force, could legally perform certain activities. Rather, to answer the legal question, one must ask who within that organization is to perform the activity and in what role will that person be acting. Because the law is fairly discrete in its application of where an individual can perform roles in more than one lane, it is important to identify the role being performed at the time of the activity in question. Extreme caution should be exercised in any potential "hat switching" and should generally only be done after appropriate legal consultation. Indeed, because the law of CND is still rather complex, persons who work in this field are advised to seek the advice of their organization's legal staff whenever they are unclear as to what is and is not legally permitted. ■

## References

1. The list is not disjunctive, as many of these categories may overlap. "Script kiddies" are inexperienced hackers who rely on pre-written attack scripts, available over the Internet, because of their own technical inabilities. Frequently they will not even understand how or why the script works.
2. 18 U.S.C. §2511(2)(i).

## About the Author

**Rick Aldrich**

Mr. Aldrich is Senior Computer Network Operations Policy Analyst for IATAC. Previously, he served as the Deputy Staff Judge Advocate for the Air Force Office of Special Investigations, specializing in the cybercrime and information operations portfolios. He has been awarded several grants by the Institute for National Security Studies and has multiple publications related to the legal implications of information warfare. He has a B.S. in Computer Science from the U.S. Air Force Academy, a J.D. from UCLA, and an LL.M. in Intellectual Property Law from the University of Houston.

# The College Cyber Defenders

By Dr. Fred Cohen

In 1998, Dick Isler and Fred Cohen founded the College Cyber Defenders (CCD) at Sandia National Laboratories in Livermore, California. The purpose of the CCD is to provide information assurance training to college students while simultaneously growing a talent pool for Sandia Labs and other government organizations. For students to be eligible for the program they must be an American citizen, studying in a computer related field, with at least a 3.0 grade point average on a 4 point grading scale. Over the past four years, the CCDs have employed over 75 students and produced numerous research projects presented to audiences ranging from White House staffers, the IEEE Computer Society, and the television show *60 Minutes*. Many of the program's former students now work for the Government on issues related to cyber security. The alumni's prototypes for high assurance Domain Name Servers (DNS), huge file systems in Linux, and deception technologies are in use around the world, and their designs have found their way into systems ranging from DoD tactical systems to bootable CD–ROMs used for digital forensics.

During its short four year life-span, the CCDs have produced numerous other research projects. These include: a digital forensics workstation and distributed forensics analysis system (60 computers) for doing large volume analysis, automated over-the-Internet intelligence collection and correlation, the first widely available database of Internet attacks tested against real systems, a network RAID array for distributed reliable file storage and retrieval, a digital diode for 100 Mbps high assurance one-way transfers, the deception wall (DWALL) for large-scale realistic network deceptions, searching the Internet to characterize useful indicators of biological attack, the Distributed Analysis and Response system for detecting correlated attacks on networks, the invisible router for large-scale tactical network deceptions, and an experimental firewall for producing resilient networking technology for defeating distributed denial of service attacks on a global scale. All of this research and development work was done on a shoestring budget—totaling less than $500,000 in student salaries for the biggest year and leveraging approximately $500,000 of other research funds to support staff salaries, equipment, and operating overhead.

Although there have been many substantial research results and spin-offs into other funded projects (such as the national Cyber Corps), the CCDs are well on their way to extinction. The original money for creating the CCDs was seed funding, and as such, it is not being used to seed other efforts. The transition from seed funding to permanent funding resulted in more "mission oriented" projects, and as a result, the CCDs mission is changing from one of research and prototypes to one of an inexpensive development team. Current projects involve implementing high performance workstations with COTS hardware and rebuilding a user interface to allow managers to view network status information. For the fall of 2002, the only research effort planned is ongoing work on deception for information protection, with research funding less than $500,000 total.

Nevertheless, it is worthwhile to focus on the substantial successes of the program. The CCDs brought the Government ten new highly trained, full-time employees in the field of cyber security. The CCDs also produced breakthroughs in several research areas, most notably in the area of network deceptions where it produced the first effective technologies in this new defensive area. The CCDs created a model program that has led to other organizations such as the Cyber Corps and similar CCD like groups throughout the nation. All of these technical accomplishments, coupled with the mentoring and training of more than 75 students in a span of four years are a remarkable set of results for such a small capital investment. ■

## About the Author

**Dr. Fred Cohen**

Dr. Fred Cohen is best known as the inventor of computer viruses and virus defense techniques. But his work on information protection extends far beyond the computer virus realm. In the 1970s he designed network protocols for secure digital networks carrying voice, video, and data; and he helped develop and prototype the electronic cashwatch for implementing personal digital money systems. In the 1980s, he developed integrity mechanisms for secure operating systems, consulted for many major corporations, taught short courses in information protection to over 10,000 students worldwide, and in 1989, he won the prestigious international Information Technology Award for his work on integrity protection. In the first half of the 1990s, he developed protection testing and audit techniques and systems, secure Internet servers and systems, and defensive information warfare techniques and systems. His more recent work in the use of deception for information protection has been widely acclaimed. All told, the protection techniques he pioneered are now used in more than three quarters of all the computers in the world.

Dr. Cohen has authored over 150 invited, refereed, and other scientific and management research articles, writes a monthly column for *Network Security Magazine* on managing network security, and has written several widely read books on information protection. His series of "Infosec Baseline" studies have been widely used by the research community as stepping off points for further research, and his "50 Ways" series is very popular among practitioners looking for issues to be addressed. His most recent "Protection for Deception" series of papers is considered seminal in that field.

Dr. Cohen holds a Ph.D. in Electrical Engineering from the University of Southern California, an M.S. in Information Systems from the University of Pittsburg, and a B.S. in Electrical Engineering from Carnegie-Mellon University.

More information on the College Cyber Defenders is available at http://heat.ca.sandia.gov/.

# Information Assurance Collection Acquistions

## *Summer 2002*

**Interactive CD-ROM**


The Information Assurance Technology Analysis Center (IATAC) provides the Department of Defense (DoD) with a central point of access for information operations and information assurance (IA) emerging technologies which include—

- Collecting, analyzing, and disseminating IO/IA scientific and technical information (STI)
- Supporting user inquiries
- Operating and expanding databases
- Promoting IO/IA current awareness activities (e.g., IAnewsletter)
- Developing technical reports

IATAC is chartered to provide DoD and government additional IO/IA support through Technical Area Tasks (TATs). The benefit of TATs is the resulting STI that becomes part of the IATAC holdings and is available to the rest of DoD/government to leverage.

This CD-ROM provides a sampling of new acquisitions specifically developed through TATs and which have a Distribution Statement of A, B, C, or D. Abstracts of STI with more restrictive distribution statements or which are classified have been included. These may be requested separately through IATAC.

Please visit our Web site at http://iac.dtic.mil/iatac/products/products.htm to order the interactive CD-ROM, available late August.


# Information Security Incident Response

## Part II: Creating an Incident Response Team

By Gordon Steele



Today's computing environments employ distributed information systems. Distributed information systems consist of six linked elements—

- Business Processes: Related groups of steps or activities that use *participants*, information, and other resources to provide *products* or *services* to internal or external *customers*
- Internal or external *customers* of the business processes
- *Products* or *services* generated by the business processes
- *Participants*: People who participate in the business processes
- *Information* the business processes use or create
- *Technology* the business processes use

Incident response is that set of actions taken *to correct* [1] an information system's failure to provide *reasonable* [2] and/or *prescribed* [3] security services that have resulted in an *information system security incident*. [4]

This mission requires incident response teams that have been organized, trained, staffed, and equipped to accomplish the mission in an effective and efficient manner. Information system security incidents may originate from, or be directed against, any combination of the elements of an information system. Thus an enterprise that utilizes distributed computing must be capable of addressing incidents caused by, or directed against, any or all of these elements. This requires a multidisciplinary approach, including not only IT and security personnel, but accountants, lawyers, human resources personnel, etc., as well. To be ready to address a particular incident means that the enterprise must be able to conduct the following activities effectively and efficiently: prepare to handle that type of incident; identify that type of incident when it occurs; contain the effects of that type of incident; eradicate the cause of that type of incident and the circumstances that facilitated it; recover the environment to a secure state; and follow-up to ensure that administrative and technical controls are adjusted to prevent future occurrences of the same type of incident. Four particularly good indicators of *operational readiness* to perform these activities are—

- Whether the enterprise is organized in a way that facilitates effective and efficient information system security incident response operations,
- Whether the enterprise is staffed with individuals competent to conduct incident response operations involving all six elements of distributed information systems,
- Whether the enterprise's incident handlers are appropriately trained and educated to conduct incident response operations in all six elements of distributed information systems, and
- Whether the enterprise's incident handlers are adequately equipped to conduct incident response operations.

Readiness to conduct these activities is a direct result of the enterprise's information security incident response program. Structuring the program is the topic of the balance of this article. Note that although the common name applied to teams that perform these services for industry and Government are *Computer* Security Incident Response Team (CSIRT) and *Computer* Emergency Response Team (CERT) respectively, most of these teams address incidents involving whole information systems, not just computers.

One good approach to building a computer security incident response capability advanced by West-Brown, Stikvoort, and Kossakowski [5] is to construct a program that breaks down the work of building the CSIRT into five phases. Each is described below—

- **Phase I: CSIRT Familiarization**—The enterprise wants to start a team but is not familiar with what a CSIRT is or does. Key stakeholders need to undertake awareness training to learn about various approaches for implementing a team.
- **Phase II: CSIRT Project Planning, Programming, and Budgeting**—The enterprise has some knowledge about CSIRTs, and is beginning to identify and

analyze the various issues that must be addressed to plan the CSIRT implementation.

- **Phase III: CSIRT Initial Operational Capability (IOC)**—The CSIRT begins to provide services. It already possesses an identified constituency, mission, and services, initial staff and training, draft standard operating procedures (SOP), and a secure infrastructure. As the CSIRT becomes adept at providing the services offered at IOC it might turn its attention to expanding its service offerings.
- **Phase IV: CSIRT Full Operational Capability (FOC)**—The CSIRT is handling incidents and has been operational for six months to a year.
- **Phase V: CSIRT Peer Collaboration**—Some techniques and operational methodologies can only be learned with time and experience. Once the CSIRT has been in existence for two years or more, and has extensive experience in incident handling, it is considered by most teams to be a mature team. By this point it has usually become a peer collaborator with other CSIRTs.

Although many enterprises start their program already offering some ad-hoc CSIRT services, most will not reach Phase IV or V of this model without designing and implementing an incident response program. Reaching these phases requires an enterprise to undertake a considered and disciplined approach, like the one above. This approach can yield effective, consistent incident response service delivery to a defined constituency. Less disciplined approaches historically do not produce this result. Thus, it is necessary for most enterprises to step back to Phase I and build their CSIRT capability properly "from the ground up." Each of the phases is described below.

## Phase I: CSIRT Familiarization

Before an enterprise can begin to build an effective CSIRT its key stakeholders must understand what CSIRTs typically do, how long it takes to establish an incident response capability, and the impact on the enterprise of establishing and operating one (including how much it is likely to cost). Key stakeholders are all those who provide, or are significantly impacted by, the CSIRT's mission performance, service deployment schedule, and/or the resources required to develop, operate, and sustain it. Since this is a substantial effort, a good start is to appoint a project manager. Ideally this individual will later become the enterprise CSIRT manager. Because the CSIRT can potentially impact the entire enterprise, the CSIRT development project manager should be positioned to have authority over all aspects of the enterprise.

It should be recognized from the onset that establishing a sustainable enterprise incident response capability is a lengthy process. If the enterprise requires some capabilities immediately then some stopgap measures should be adopted in the interim period. These could include contracting with a commercial CSIRT until an in-house capability is established, or establishing a "virtual team" of senior computer engineers that begin to focus on providing an immediate capability. These persons would be better positioned to deal with an incident than an ad hoc capability, but not as capable as teams that are organized, trained, staffed, and equipped through this program. As a group these persons should be at a minimum, competent in system, application, and network engineering for all hosts in the environment; be familiar with evidence preservation requirements; command the respect of management; and demonstrate hands-on technical competence in their respective discipline.

## Phase II: CSIRT Project Planning, Programming, and Budgeting

Once the decision is made to proceed with standing up a CSIRT, a number of activities must be accomplished. Each activity is described below—

1. Gather information about information systems, both deployed and planned, for the operational environment
2. Develop the CSIRT frameworks
3. Identify personnel, equipment, and infrastructure resources
4. Determine CSIRT reporting structure, authority, and organizational model
5. Create, socialize, and obtain approval for a CSIRT program plan
6. Secure funding for CSIRT operations
7. Procure personnel, equipment, and infrastructure resources
8. Announce the CSIRT, and in so doing, communicate its mission and services

Four organizational frameworks must be built on which the CSIRT will base much of its ability to function effectively. Again, building on the work of West-Brown, Stikvoort, and Kossakowski [6], they are—

- **Operational Framework**: Identifies and or defines statement of vision, clearly defined mission, achievable goals, defined constituency, organizational home, and formal relationship to other teams.
- **Service and Policy Framework**: Defines the range and levels of services to be offered; describes information flows into/within/out of the CSIRT; defines processes for collecting, recording, tracking, and archiving information; provides clear, comprehensive enterprise-wide incident response policies; segments the overall mission into logical mission areas, or services; envisions profiles of potential incident response scenarios; identifies the capabilities (functions) required to fulfill each mission area; and builds a work breakdown structure (WBS) for each service area which has, at it lowest level, a listing of all the activities the CSIRT must be able to perform in order to provide each required capability. This list of activities will serve as the basis for identifying the equipment and skills required to perform each activity. The resulting lists of equipment and skills provide a basis for developing the CSIRT inventory, as well as organizational structure and training requirements.
- **Standards, Guidelines, and Procedures Framework**: Identifies and/or defines standards, guidelines, and procedures that will be used by persons performing the incident response mission. Standards describe mandatory methods for performing a function whereas guidelines describe recommended methods for doing so. Procedures are cited within standards and guidelines and are keystroke

*…continued on page 21*

# Space-Based Blue Force Tracking

By LTC Timothy J. Sutlief, USA

## The Deadly Fog of War

### July 3, 1863

If Robert E. Lee had known where his "eyes and ears" cavalry commander, J.E.B. Stuart, was while approaching Gettysburg, would he have directed Pickett's charge up a hill into a Union Army protected by a stone wall?

## Poor Command and Control

### December 7, 1941

If young American radar operators on a north Oahu hilltop had the capability to locate American B–17 bombers flying in from California, would they have realized the radar returns weren't friendly B–17s, and alerted resting battleship crews?

## Inadequate Situational Awareness

### August 14, 1991

The Pentagon reports that of 148 American fatalities in the Gulf War, 35 were killed by American friendly forces—including 16 attacks by U.S. ground forces on U.S ground forces, and 9 attacks by U.S. aircraft on U.S. ground forces. How do we eliminate combat fatalities caused by friendly fire?

## Fratricide

### June 6, 1995

After four days behind enemy Serbian lines, U.S. Air Force F–16 pilot, Captain Scott O'Grady, reaches a Bosnian hilltop to radio his location and is subsequently rescued by a Marine helicopter. If he would have had Space-Based Blue Force Tracking (SB–BFT), might he have been rescued within hours of his June 2 shoot-down?

## Delayed Personnel Recovery/Combat Search and Rescue

### October 10, 2001

United States Space Command (USSPACECOM) declares initial operating capability of the SB–BFT Mission Management Center (MMC) supporting combat operations in Afghanistan. IATAC personnel—guiding its formation and designing a future worldwide DoD architecture—man the MMC's controls around the clock. The "War on Terrorism" is underway.

## The Assignment

### Beginning

In June 1996, IATAC personnel were selected to support the Space Exploitation and Integration Branch (J33T), Space Exploitation and Force Enhancement Division (J33), Directorate of Operations (J3), HQ, USSPACECOM, Peterson AFB, Colorado. The J33T organization is charged with identifying opportunities to make emerging space systems more relevant to theater Military operations. From 1998 through early 2000, USSPACECOM, in close partnership with IATAC staff, acted as the Executive Agent for the Joint Staff's Special Project series. Joint Staff Special Project 99, "Operation Southern Eye," integrated 16 space-related capabilities to enhance asymmetric warfare. One of the technologies in the demonstration was SB–BFT. SB–BFT is the ability to automatically report the precise location, movement, and status of friendly (blue) assets (people, vehicles, aircraft) to a command and control headquarters via spacecraft. While this capability had been technically proven already, the SP–99 project highlighted the need to make SB–BFT operationally relevant to the larger DoD force. In March 2000, the USSPACECOM/IATAC team saw the need to "operationalize" this capability, and initiated the development of a Concept of Operations (CONOPS) for SB–BFT. This CONOPS document established the baseline both for today's initial operational capability and for a

future architecture that will fundamentally change the future nature of military operations.

## Military Missions

Throughout the history of warfare, commanders have given high priority to operating procedures and communications technologies that help them—

- Avoid fratricide in the heat of battle
- Succeed in combat search and rescue
- Control clandestine special operations
- Recover personnel inserted deep in enemy territory
- Maintain situational awareness of all forces and visualize the battlefield
- Assess battle damage
- Track logistics movement, among other missions.

This has become even more urgent with the recent advent of high-speed, long-range weapons allowing reliable pinpoint accuracy.

## Technology Jumps Ahead of Organization

In 1990, newspapers wrote of American soldiers deploying to Desert Shield with brand-new Global Positioning System (GPS) receivers they bought at Radio Shack—before the DoD set common standards for use of this emerging capability and began officially procuring GPS receivers as standard equipment. During the late '90s, as commercial trucking companies began tracking their cargos by satellite nationwide, the Military Services began procuring a variety of disparate commercial equipment to track DoD forces. This again has caused a proliferation of non-integrated capabilities serving niche requirements without a clear roadmap for the future. DoD is struggling with this dilemma today.

## Thinking Ahead of Technology

Lest the taxpayer end up paying five-fold for the same technology in many different boxes, the USSPACECOM/IATAC team took the initiative in 1999 to characterize the SB–BFT requirements of the Military Services and the global combatant commanders. Upon consolidating these requirements, and with the guidance of the DoD Joint Requirements Oversight Council (JROC), the team laid out a conceptual operational mission flow, technical and operational standards, technical development and implementation plan for the systems architecture, user training plan and funding advocacy to operationalize SB–BFT to address the holistic needs of the warfighting community.

## IATAC Takes the Lead

USSPACECOM began coordinating its intent and vision to begin this important global mission—two years before September 11, 2001.

In 1999, following the warfighting community's acceptance of the IATAC-developed SB–BFT CONOPS document, USSPACECOM began to contemplate the task of building the SB–BFT MMC in Colorado Springs. The MMC, once transitioned to Army Space Command when complete, would become the global operations center for conducting Blue Force Tracking operations and notifying warfighting commands of critical force movements.

The IATAC Team provided support, initial personnel, and expertise for MMC implementation. The IATAC role included overall information assurance (IA) strategy, development, and implementation of a funding approach, and construction of an implementation plan. Execution of the funding approach required coordination through, and approval by, the Chairman of the Joint Chiefs of Staff, General Hugh Shelton.

In September 2000, General Shelton approved a $3.366M Commander in Chief Initiatives Funds (CIF) request from Vice Admiral Herb Browne, the Unified Deputy Commander of USSPACECOM, to implement the SB–BFT MMC.

IATAC provided task leads and other personnel for each of the four pillars of the MMC implementation task: system development, test and evaluation, warfighter integration, and operational transition.

## Making a Difference

Throughout 2001, the MMC supported several major Military exercises including the Courageous Channel (CC) and Reception, Staging, Onward Movement, and Integration (RSOI) exercises for U.S. Forces-Korea, as well as the Cobra Gold exercise for U.S. Pacific Command.

Additionally, the MMC, including its IATAC staff members, accomplished significant operational planning with the intent to support the Bright Star exercise in Egypt scheduled for October 2001. The attacks of September 11, 2001 precluded the MMC's participation in Bright Star, thrusting the team into around-the-clock operational support for the War on Terrorism.

After September 11, the MMC's operational development and technical architecture integration were accelerated. On October 10, 2001, USSPACECOM declared initial operational capability for the MMC and initiated its support for forces executing Operation Enduring Freedom in Afghanistan.

## Stepping Up to War

Today, IATAC staff ensure that the SB–BFT IA architecture tracks high-value blue force assets in many areas around the globe. The MMC facilitates theater support requests by coordinating them through existing Intelligence Community channels. SB–BFT data is disseminated to combat headquarters and joint task force commanders, providing the requested battlefield situational awareness. Lieutenant General Cosumano, Commander of the Army Space and Missile Defense Command (SMDC), highlighted the significance of this new capability in an interview with *Defense Daily* on February 26, 2002—

> *Many new space-based technologies…have played a critical role in the war in Afghanistan and demonstrated use of space as a critical enabler for future battlefields…a new Blue Force Tracking system…was used in Afghanistan. I think it's safe to say the kinds of technologies driven by computers and sensors in space are becoming more key.*

LTG Cosumano predicts that SMDC space capabilities and expertise will become "a key enabler across the full spectrum of forces" in providing "constant battlefield awareness and use of precision guided munitions to a higher degree."

*What we are seeing for the first time in our space capabilities is the impact of space on the battlefield.*

After utilizing the existing SB–BFT capability in Operation Enduring Freedom, four major combatant commands have released urgent BFT combat mission need statements for additional capability to track such things as vehicles, airdrop bundles, individual soldiers operating on the ground, and downed aircrew.

### And Beyond

In the future, the MMC will become the single point of contact for SB–BFT support to warfighting units. The migration to a fully-dedicated DoD IA architecture will include—

1. Accepting request coordination and planning process responsibilities
2. Working with functional managers for BFT DoD satellite payloads
3. Moving toward the goal of having a BFT payload on every satellite.

Dissemination will be to the lowest levels of each requesting echelon (i.e., individual aircraft cockpit). Situational awareness capabilities will be integrated into a global shared situational awareness architecture and embedded in all communications and navigation capabilities envisioned for DoD forces.

### Teamwork

Realizing the full scope and inevitable impact of the BFT capability on Military operations, the USSPACECOM/IATAC integrated team has worked extensively with stakeholders across the DoD. The team has seamlessly engaged on issues traversing the scope of BFT implementation, from current operations support to long-range IA architecture planning and policy.

### Intellectual Capital

Unique intellectual capital has been developed in three key areas: visioneering, transition to operations, and operations support. The IATAC team—

- Has captured a unique cross-BFT stakeholder view of the vision, strategy and approach for the objective BFT capability not held uniquely by any individual or subgroup of stakeholders
- Has developed a repeatable process for transitioning niche space technology applications to broader military operational relevance
- Is building current operations support experience.

### Groundbreaking Innovation

As the IATAC Team developed the MMC, USSPACECOM executed a SB–BFT analysis of alternatives (AoA) that examined broad SB–BFT mission area requirements, stakeholders, transmitters, commercial systems, and existing on-orbit satellite capabilities. This study effort enabled USSPACECOM to make key recommendations in an August 2001 presentation to DoD's senior leadership. As a result, USSPACECOM was named "Lead Command" for SB–BFT, and a partnership with U.S. Joint Forces Command and U.S. Special Operations Command was formed for BFT mission area development.

### Extending the State-of-the-Art

While migrating satellite support for the current small number of commercially-procured BFT transmitters in the DoD, and while providing warfighter support today for the War on Terrorism in Afghanistan, the most significant contribution of IATAC in the art and technology of BFT is the design and construction of an integrated global IA architecture for the future. It is upon this architecture that future satellite designs will incorporate BFT equipment, and it is within this architecture that the various Military Services and global combatant commands will procure and employ tens of thousands of interoperable, integrated BFT transmitters and receivers that must work together seamlessly. This is not the designing of hardware, but the designing of the global IA architecture and satellite communications hardware and software into which the individual soldier's equipment will be designed to fit.

### Openings to New Uses

As made clear in the IATAC BFT Team's discussions with Military and commercial clients and partners, as well as with many internal service teams, the customer base for effective, timely BFT service is growing quickly. One need only to look at the explosive growth in the utilization of GPS to understand the fundamental impact of BFT across many facets of theater military operations as well as commercial industries around the globe. For example, a recent survey of eight U.S. Air Force major commands found BFT requirements in six of these spanning five separate missions areas—and often ranked in their top three requirements.

## Working With the Warfighter

### Doing What's Best

While sitting side-by-side with the warfighter providing SB–BFT support to fielded combat units, the IATAC Team continues to develop needed software, standard operating procedures, tactics, techniques, and training materials to help the user become more efficient and effective. This flexible, results-oriented teamwork is ongoing right now.

### Senior Leadership Involvement

The SB–BFT effort has visibility at the highest levels of the Department of Defense.

Leading the August 2001 SB–BFT presentation to the Joint Requirements Oversight Council (JROC) was Lieutenant General Edward G. Anderson, U.S. Army, Deputy

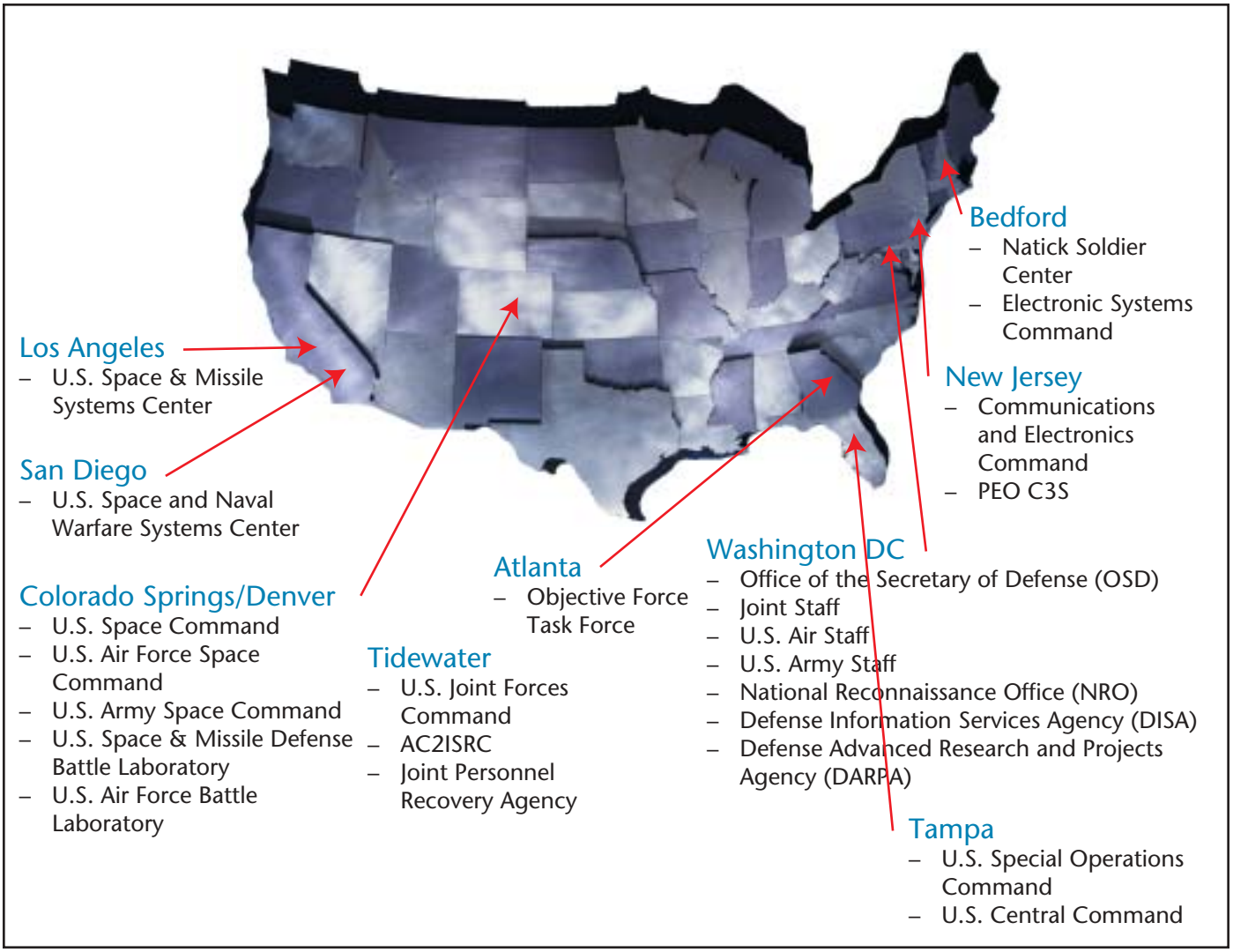



**Figure 1. Blue Force Tracking Stakeholder Engagements**

Commander, USSPACECOM. General Richard B. Myers, U.S. Air Force, then Vice Chairman and now Chairman of the Joint Chiefs of Staff, chaired this JROC.

With General Myers on the JROC were the Vice Chiefs of the U.S. Air Force, U.S. Army, and U.S. Navy, and the Assistant Commandant of the U.S. Marine Corps. Also attending were Lieutenant General William P. Tangney, Deputy Commander, U. S. Special Operations Command; Rear Admiral Robert Nutwell, Deputy Assistant Secretary of Defense for Command Control Communications and Intelligence Surveillance Reconnaissance & Space; and Dennis Fitzgerald, Deputy Director of the National Reconnaissance Office. The resulting JROC memorandum noted that SB–BFT has "tremendous potential," and directed U.S. Space Command to partner with U.S. Special Operations Command and U.S. Joint Forces Command to develop a broad-based operational concept to track friendly forces and logistics, and to investigate broader BFT utilization.

## Intellectual Beginnings and Scoping

In the late 1990s, DoD was driven to address the need for an integrated DoD BFT architecture—by the confluence of two forces—

1. DoD and National Intelligence Community policy guidance limiting future Intelligence Community collection and dissemination support; and

2. Accelerating procurement of a variety of commercial systems by the various Military Services, making obvious the potential for duplicative spending and lack of interoperability.

Related systems being procured by the Military have included Qualcomm's OmniTRACS, Comtech Mobile DataCom's Mobile Tracking System (MTS), Iridium's PocketCOP, the Army's Grenadier BRAT, the Air Force's Combat Survivor Evader Locator (CSEL) radio, and the Navy SEALs' Lynx system.

To manage this pervasive mission need within its approved management systems, DoD found itself with evolving technologies (wave forms, radios, architectures) and a large and growing stakeholder community wanting BFT—with each of the Military Services already working on service-unique user systems.

However, community leadership was disengaged. DoD had no independent capstone requirements document, no operational requirements document, no DoD executive agent, no lead service, no interagency stakeholder commu-

nity coordinator, no functional manager for DoD BFT, and no joint center of excellence. Therefore, no central point of contact was available to—

1. Evaluate emerging technologies
2. Provide technical expertise on system architecture options
3. Establish joint technical standards
4. Share lessons-learned
5. Draft joint doctrine, joint policy, joint long-range plans, joint procedures, and joint threat assessments
6. Provide operational planning, exercise, and hot contingency assistance to combatant commanders
7. Advise on funding and procurement options
8. Advocate and educate on the soon-to-be-pervasive BFT capability.

This was the environment into which, in June 1999, USSPACECOM contracted with IATAC to develop the SB–BFT CONOP document, which ultimately established the baseline for today's joint operational capability and tomorrow's seamless architecture.

## Excellent Execution

The immediate task of designing and engineering the MMC was a matter of spiral development—iterative and simultaneous. The IATAC Team defined MMC requirements, operational flows, system hardware, and software design using an IATAC team member's-developed mission engineering process, then created a multi-media model of the user interface. The USSPACECOM and IATAC Team members encouraged the involvement of a multi-discipline team of engineers, software developers, warfighter customers, and test and evaluation experts during each iteration, as well as advising USSPACECOM on potential sources and pacing of funding.

This spiral development continues, with an excellent execution milestone marked on October 10, 2001, when demands to support the War on Terrorism drove accelerated declaration of MMC initial operating capability three months earlier than planned, along with 24-hour operation including IATAC personnel on shift.

As written in February 2002 by Rear Admiral James D. McArthur, Jr., Director of Operations, HQ USSPACECOM, "This center (MMC) provides a new and significant capability for Warfighters throughout the DoD."

## World-class Intellectual Capital

The now-operational MMC acts as a conduit between the warfighter and BFT support providers, using a global IA architecture to assure that requested support is provided in a thorough, timely fashion. In order to accomplish this, the integrated USSPACECOM/IATAC team has built partnerships among the DoD, National Intelligence, Civil Government Space, and Commercial Space and communications communities, as well as with each Military Service and combatant command headquarters worldwide.

While conducting daily operations in concert with this large set of partners, including support to combat missions, USSPACECOM and its IATAC Team are pursuing improved operating procedures, new technologies, improvements to legacy space systems, and BFT requirements to be built into future space systems. This effort includes support to joint deliberate and crisis planning conducted by the combatant commanders, exercises, and demonstrations, and advocacy for investments such as robust geosynchronous satellite BFT capability.

## Decisions For the Future

USSPACECOM intends to further develop the SB–BFT MMC into a one-stop shop for fully-automated BFT support to combatant commands worldwide. To provide assured support at any time and real-time update of needed information, using a robust satellite capability—within an integrated, seamless global IA architecture managed by USSPACECOM.

Not willing to rest on past successes, and with a desire to continue the innovation process, the BFT team has proposed enhancements to the MMC that would be developed and evaluated in the Space Warfare Center. The IATAC Team is confident that the SB–BFT mission will greatly expand, especially since SB–BFT is key to the full realization of the *Joint Vision 2020* mandate as published by the Chairman of the Joint Chiefs of Staff.

The work necessary to accomplish the BFT mission will require the kind of intellectual capital, operational continuity, and broad stakeholder community reach provided so effectively by IATAC to USSPACECOM today. ■

## References


1. "Improved Military Space Key to Antiterrorism War," *Aviation Week & Space Technology*, December 10, 2001.
2. "Space and Missile Defense Command Capabilities Proven in Afghanistan" *Defense Daily*, February 26, 2002.
3. "Building New Business By Building New DoD Capabilities: The Space-Based Blue Force Tracking Story," *Intelligence Quarterly*, March 2002.


## About the Author


**LTC Timothy J. Sutlief**

LTC Timothy J. Sutlief, U.S. Army, is currently serving on a Joint tour with USSPACECOM, Peterson AFB, CO. He is the Chief, Space Exploitation and Integration Branch, within the Space Exploitation and Force Enhancement Division, Directorate of Operations. LTC Sutlief holds a Master's Degree in General Administration from Central Michigan University in addition to a B.S. from Missouri Western State College. His Military schools include the Military Intelligence Officer Basic and Advance courses, and Command and General Staff College. LTC Sutlief can be reached via E-mail at timothy.sutlief@peterson.af.mil or by phone at 719/554-5955.

*…continued from page 15 (Information Security Incident Response, Part II: Creating a Incident Response Team)*

level descriptions of how to perform particular activities required by standards and guidelines.

- **Quality Assurance Practices**: Provides a definition of a quality system; specific measurements and checks of quality parameters; reporting and auditing practices and procedures; balance, compliance, and escalation procedures to ensure quality levels; and constituency feedback.

At this point, using the frameworks identified above, the CSIRT development project manager must identify personnel, equipment, and infrastructure resources suitable to implement each framework. A CSIRT reporting structure, authority, and organizational model must be identified. A CSIRT program plan should be created, socialized, and approved by the chief executive of the enterprise. Once the plan is approved, funding for CSIRT operations must be secured. Once funding has been secured, personnel, equipment, and infrastructure resources should be procured. Only after all these activities have been accomplished should the CSIRT announce itself to the constituency, and in so doing, communicate its mission and services.

## Phase III: CSIRT Initial Operational Capability

The CSIRT is now ready to begin formal operations. This is the point at which the CSIRT can declare that it has reached an initial operational capability (IOC). Some CSIRTs will add services in a phased manner starting only with incident handling and later adding services such as forensics, advisory services, artifact analysis, etc. Once the basic incident handling service is being provided it is a good time to undertake projects to provision these additional services.

## Phase IV: CSIRT Full Operational Capability

Once all services are in place and functional and the CSIRT has provisioned all services called for in the program plan, and is providing all services at the desired level of performance, the CSIRT has reached full operational capability.

## Phase V: CSIRT Peer Collaboration

At this point the CSIRT has been involved in numerous incident response operations and is recognized by other incident response team as a trusted member of the community. Typical time to reach this point is about two years from the start of the effort, if the organization proceeds in earnest throughout the effort. ■

## References


1. "To correct" implies: resumption (or commencement) of effective security services; recovery (as much as possible) of losses sustained; prevention of further loss attributable to security events, attacks, and incidents of a similar nature, and pursuit of those agents, and persons, that exploited that security failure.
2. Reasonable security services are commonly accepted as those that should be provided by security architecture, such as those named in the OSI security architecture. Specifically, these include: authentication, access control, data confidentiality, data integrity, and non-repudiation. To these is frequently added system availability in the face of attack. It also includes those security services that are recognized by the information security community as best practices.
3. Prescribed security services are those required by enterprise security policies and/or by public law, government regulation, contractual obligation, or administrative rule (all of which should be incorporated into the enterprise's security policy framework).
4. "Information system security incident" is defined according to the taxonomy presented in Howard and Longstaff, "A Common Language for Computer Security Incidents", Sandia National Laboratories, 1998. http://www.cert.org/research/taxonomy_988667.pdf
5. West-Brown, Stikvoort, Kossakowski, *Handbook for Computer Security Incident Response Teams (CSIRTs)*, Carnegie-Mellon University Software Engineering Institute, December 1998.
6. Ibid.


## About the Author


**Gordon Steele**

Mr. Gordon Steele is the Deputy Director of IATAC. He may be reached at iatac@dtic.mil.


*…continued from page 9 (GIG Interconnection Approval Process (GIAP))*

your connection approved because the Certification, Testing, and Evaluations (CT&Es) for the devices listed have already been completed. This will cut the process time on average to less than one year (as little as 3 months in some cases), as opposed to three years or greater for unknown solutions. You will also find System Security Authorization Agreement (SSAA) templates, SABI and DISN Security Authorization Working Group (DSAWG) (the final approving authority for SABI implementations) case law and minutes, and a condensed SABI customer guide that will explain the process in greater detail. It is all there to help you get through the process as quickly as possible.

In addition to the resources on the GIAP Web site, we have created to the "GIAP Toolbox" in support of Information Assurance ET&A. The Toolbox is a resource kit that you can take to your desk that will provide you with the knowledge you need to get through any connection process currently supported. It includes twelve interactive CDs and all the contact information (phone numbers, email addresses, and web sites) necessary for your connection request. The GIAP toolbox is available for free from the SCAO.

The GIAP Web site can be found at http://giap.disa.smil.mil on SIPRNET. Keep this address handy, because for all future connection requests, the GIAP will be your path to approval. It was created for you, the customer, to end all the confusion and save you time and money in getting you connected to vital systems in time to meet your requirements. ■

By Chad Tilbury, AFOSI Detachment 110

# BlackBerry Security in a Military Environment

*The views expressed herein are those of the individual author. They do not purport to express the views of the Air Force Office of Special Investigations, the Department of the Air Force, or any Department or Agency of the United States Government.*



BLACKBERRY WIRELESS EMAIL SOLUTION

by Research in Motion (RIM) is currently one of the leading solutions for wireless E-mail connectivity. It is gaining prominence throughout the DoD by allowing mobile users to have access to their E-mail, appointments, and contacts, both in and out of the office. It can be used as a standalone system from a desktop computer or installed as part of the network in the enterprise version. BlackBerry acts as an always-on wireless modem which can be set to continually receive any combination of E-mail that a user is sent (push technology). The user can send and receive E-mails as well as use the unit in an off-line manner to communicate directly with other BlackBerry users. Due to its wireless nature and access to many sensitive, but unclassified networks, it would be remiss not to examine the security issues involved.

Unlike many of the IT products out today, BlackBerry was designed with security in mind. It purposefully provides confidentiality of sent messages and contains additional features to assist with the security of the handheld, if compromised. Its most prominent feature is the end-to-end encryption of messages using the Triple Data Encryption Standard (3DES) algorithm. BlackBerry is password protected and programmed to erase its contents after 10 unsuccessful login attempts, effectively preventing a classic dictionary attack. The handheld smartly uses a hash to store the user's password and the virtual private network (VPN) it creates only requires an outbound initiated connection through the network firewall. However, like many security components in a network architecture, it is not always front-line bastions which define the effectiveness of a solution. In this case, a combination of user choices and overall design combine to potentially create serious concerns for our military networks.

## Security Concerns

*BlackBerry security is completely dependent on user diligence.*

## Handheld and Standalone Security

It is well known in information security that ease-of-use and degree of protection are mutually exclusive. Passwords are an every day annoyance for computer users, yet are accepted due to the security they provide to the system. Given a choice, most would opt to limit the restrictions that information systems require. This is exactly why users should not be responsible for security and one of the primary reasons that Military desktops are switching to technologies which allow the administrator a finer granularity of control, such as Windows 2000. Unfortunately BlackBerry does not fall into this category.

The BlackBerry setup in standalone mode is surprisingly simple. First, a software package called Desktop Re-director is installed on the user's desktop computer. E-mail, appointment and contacts filters are then set up to determine which items will be transmitted to the handheld. The BlackBerry is then synced with the computer and registered with the wireless network provider. Finally, the desktop software uses the Microsoft Outlook client and redirects messages to the handheld through the Internet and via the BlackBerry Message Center (see Figure 1).

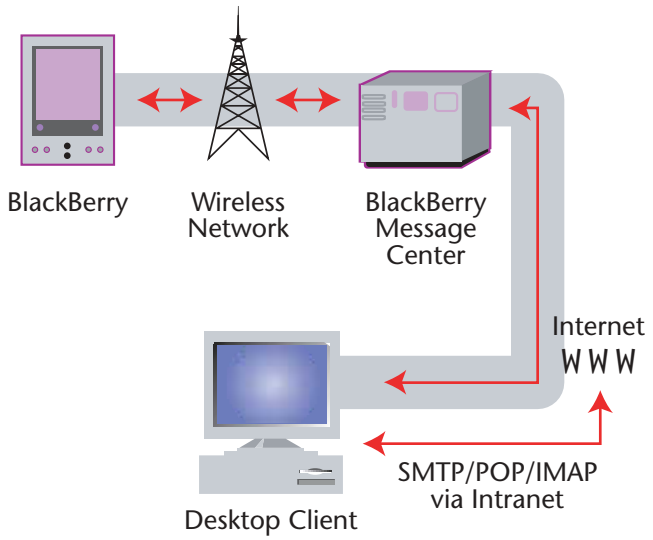



**Figure 1. The Desktop Re-director/Standalone Network Setup**

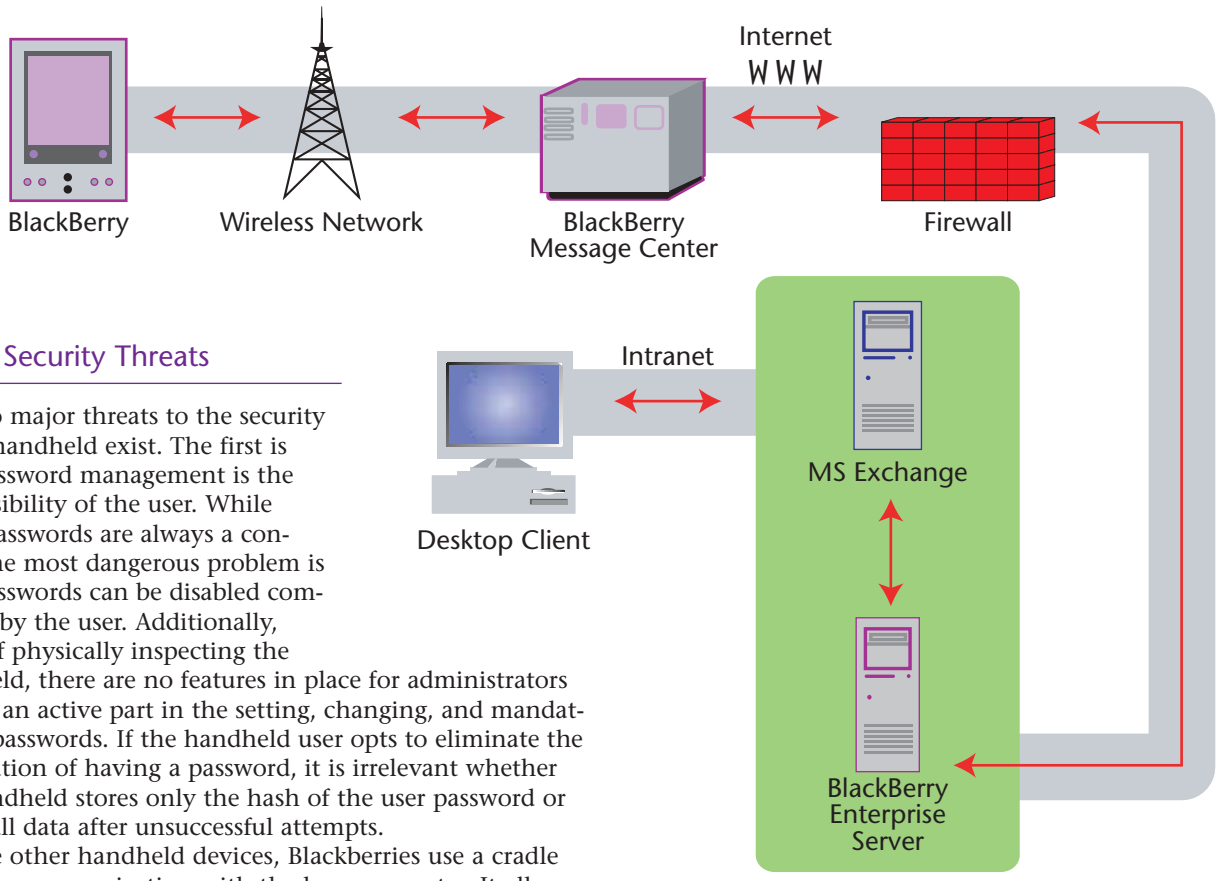



**Figure 2. Configuration of the BlackBerry Enterprise Edition**

## Major Security Threats

Two major threats to the security of the handheld exist. The first is that password management is the responsibility of the user. While weak passwords are always a concern, the most dangerous problem is that passwords can be disabled completely by the user. Additionally, short of physically inspecting the handheld, there are no features in place for administrators to play an active part in the setting, changing, and mandating of passwords. If the handheld user opts to eliminate the aggravation of having a password, it is irrelevant whether the handheld stores only the hash of the user password or erases all data after unsuccessful attempts.

Like other handheld devices, Blackberries use a cradle for bulk communication with the base computer. It allows databases to be synced and large amounts of data to be transferred quickly. In this case, it also opens up a severe security hole. The BlackBerry software is set up to switch communications to any handheld present in the cradle, with virtually no impediments. This means that any random BlackBerry can be inserted into the cradle of an unattended computer and become its new destination device. For this attack to work, the computer must be logged onto the network and not protected by a screen-saver password or other device. In addition, since Blackberries can be purchased at your local electronics store, it doesn't even have to be an authorized user of the equipment. Anyone who can bluff their way into an office can quickly configure their BlackBerry to receive another user's E-mail. This type of attack persists until the legitimate user discovers they are no longer receiving E-mails.

## Minor Security Threats

A consistent problem encountered with the BlackBerry technology is its lack of accountability. There are very few opportunities for logging or authenticating. Other than the password on the device itself, there is no additional authentication into the network E-mail system. If the unit does not have an assigned password, it is impossible to determine who is actually using the handheld. This affects both the confidentiality and integrity of the messages sent and received by the units.

The lack of logs is also a problem when using the BlackBerry to BlackBerry messaging capability. This feature allows two users with Blackberries to communicate directly with one another, circumventing the home network. This feature has already been documented by RIM as an insecure means of communication due to its use of a simple data mask as opposed to the 3DES encryption. The security company @Stake [1] recently published an attack for this mode where they were able to capture and decode the communications using a scanner and freely available software. In addition to this, there is no way for the security administrator to keep track of these communications. The only records exist at the contracted wireless provider, where a court order would be required to retrieve them. It is possible, albeit difficult, for the security administrator to turn off the capability completely, but this undermines their usefulness in emergency situations when the network may be unusable.

A final security issue with the handheld device is that the data on it is stored in an unencrypted format. While it may not even be an issue if the BlackBerry is used without a password (the data would already be accessible), it does open up the possibility of brute force attacks on the handheld to determine its contents.

## BlackBerry Enterprise Edition

The enterprise version of BlackBerry is the configuration that most Military installations are utilizing (see Figure 2.) In this configuration, a BlackBerry Enterprise Server (BES) is established as part of the base network and is used to interface with the Microsoft Exchange Server that is responsible for E-mail communications. The BES maintains a constant TCP/IP VPN connection with the RIM wireless network. It then routes messaging traffic between Exchange and the wireless handheld using the 3DES encryption algorithm. It should be noted that all of the vulnerabilities explored in

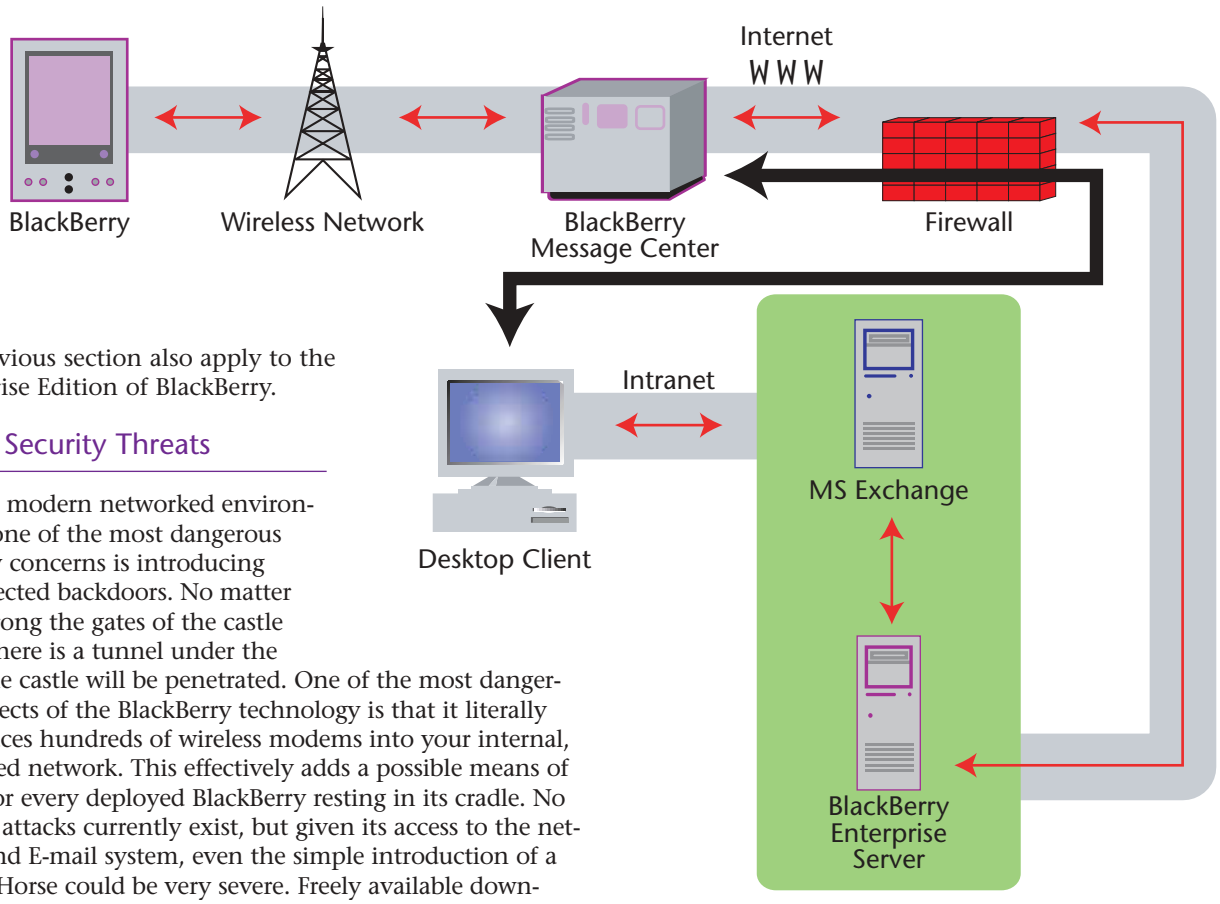



**Figure 3. Foreign BlackBerry Introduction into an Enterprise Network**

the previous section also apply to the Enterprise Edition of BlackBerry.

## Major Security Threats

In a modern networked environment, one of the most dangerous security concerns is introducing unprotected backdoors. No matter how strong the gates of the castle are, if there is a tunnel under the wall, the castle will be penetrated. One of the most dangerous aspects of the BlackBerry technology is that it literally introduces hundreds of wireless modems into your internal, protected network. This effectively adds a possible means of entry for every deployed BlackBerry resting in its cradle. No remote attacks currently exist, but given its access to the network and E-mail system, even the simple introduction of a Trojan Horse could be very severe. Freely available downloads of games and other BlackBerry software on the Internet could easily be used as a vector to infect these devices. As the proliferation of remote Windows attacks and utter lack of Apple Macintosh vulnerabilities shows, the more ubiquitous the technology, the greater the scrutiny; and greater scrutiny means a higher likelihood of finding chinks in the armor.

The lack of useful logging by BlackBerry is even more serious in an enterprise environment. Administrators rely on logs as both a preventative and detective control on network compromises and general malfeasance. The only effective logging of sent messages is at the exchange server itself. Since the BES only deals with encrypted traffic, there is no way for it to audit the receiver or content of the messages. For example, if a policy is enacted to restrict the sending of E-mail to users outside the base intranet it is difficult if not impossible to audit. Worse yet, since logging at the exchange server is often disabled due to the sheer volume of traffic, there often will be no logs at all.

The final major security issue in an enterprise environment is that of foreign BlackBerry introduction. This involves a user buying a "personal" BlackBerry at a local electronics store and attaching it to his Government computer. While there are procedures in place to prevent that user from utilizing the BES, there are no available restrictions to stop the user from using the desktop redirector software that comes with the unit. This software binds to the Microsoft Outlook program on the desktop and performs the same functions of the BES, utilizing the email infrastructure of the network to redirect messages to the handheld. Thus, even if a certain network was denied BlackBerry devices due to the sensitivity of its information, a user in the unit could opt to purchase his own. Worse yet, unless the system administrators were actively looking and blocking such an event, there is no impediment to using the government network to transmit sensitive email to the wireless handheld (see Figure 3).

## Minor Security Threats

BlackBerry uses the 3DES encryption algorithm, which is widely used and generally accepted to be very secure. An interesting part of the BlackBerry wireless network configuration is that every packet is routed via the RIM servers in Toronto, Canada. Since 3DES encryption is used end-to-end, the confidentiality of the contents of messages should be secure. However, to date there has only been one independent published analysis of BlackBerry. [2] According to the National Institute of Standards and Technology (NIST), the BlackBerry crypto system is only validated at the lowest level, FIPS 140–1 level one. Since the RIM servers are setup as store-and-forward points, it is possible for BlackBerry messages to be archived for possible future decryption.

The last minor threat is that user's symmetric encryption keys for the handheld devices are stored at the Exchange Server in a hidden folder. Since keys are generated infrequently, a nefarious system administrator could download all of the keys for the devices and use them to decrypt captured wireless traffic. The security company @Stake proved that the BlackBerry wireless traffic is easily captured which makes this a real possibility. However, it should also be noted that a System Administrator with those same permissions could just as easily access every-

one's individual email accounts to read the email there. The vulnerability lies in having the keys for future use and possibly passing them to a third party.

## What Is Jeopardized?

*BlackBerry is saved by its limitations.*

One thing that often gets overlooked in information security is the analysis of what we are protecting. Extreme countermeasures for obscure vulnerabilities may be completely unnecessary if the data itself does not need protection. For some BlackBerry implementations this may be the case. A reality check is necessary to determine what the information to be protected is and how vulnerable it is to one of the attacks discussed in previous sections.

For the most part, unique data on BlackBerry devices is limited. The average device stores copies of E-mails that are still located at the home exchange server. While on the wireless network, a BlackBerry unit is constantly syncing its data with the desktop computer. Therefore, if a unit gets lost or stolen, usually no data is actually irretrievably lost and damage assessment is easy. Additionally, in the default mode, E-mail attachments are not accessible to the handhelds. Third party software must be loaded on the enterprise to enable this feature. Since experience has shown that a majority of the E-mail security violations involve attachments, this does provide some level of protection and limits what could be compromised. An interesting thought problem is how to handle a security incident involving classified information passed via a wireless network which guarantees that the message has traversed and been stored on public networks.

This analysis also begs the question of what type of network the units are employed on. It should be obvious that these units should not be placed on classified networks. They are most suited to unclassified networks which could sustain a leak of internal email traffic. Since most military networks are considered Sensitive But Unclassified (SBU) or are configured as VPNs there is a considerable gray area. A decision must be made as to what level of protection the data requires, and what countermeasures will ensure this level is reached.

## Solutions

My intent in this article has not been to proselytize against the use of BlackBerry. On the contrary, I have merely sought to point out possible problem areas with the use of the devices in a Military environment. The following section will now attempt to provide solutions to some of these security risks in hopes of mitigating the problems.

The following are some relatively easy to implement solutions for many of the associated BlackBerry security problems—

- User agreements
- Disable wireless modem when cradled
- Enforce password protected screensavers for users
- Disable BlackBerry to BlackBerry at the server

User agreements should be standard with any piece of IT equipment, but particularly so with Blackberries. As mentioned above, security on these devices is in many cases left up to the individual users. The only way to enforce your security policies on these systems is to maintain and enforce signed user agreements. Built in to the agreements should be the standard DoD warning banner, consenting to monitoring at any time. Disabling the BlackBerry wireless modem when cradled should also be standard. This is an available feature of the units, but must be manually implemented each time the unit is placed in the cradle. Since no logging or auditing hooks exist for this, the requirement should be addressed in the user agreement.

Passwords for the handhelds should also be mandatory. If a BlackBerry is password protected, a screensaver is enabled on the desktop system when mail is being directed to it. Since passwords cannot be enforced and can only be effectively managed by user agreements, an option to consider is to force password protected screensavers for all Windows machines. This can be implemented in Windows 2000 through the Active Directory structure. This countermeasure will prevent the cradle attack method used to unwittingly send email to a rogue BlackBerry.

To stop the foreign Blackberry introduction attack, administrators need to block outgoing mail to the E-mail address "network@blackberry.net." This can be accomplished at the mail server or at the firewall security perimeter and effectively prevents the Blackberry Desktop Redirector software from communicating with the Blackberry Message Center. A final countermeasure is to disable peer-to-peer use of the handhelds at the network level. The BlackBerry Enterprise Server does come with the capability to do this via the policy.inf file. However, it is somewhat of an extreme measure since it will prevent the units from this mode of communication at all times. This means in the event of a catastrophe or base network outage, the units will be effectively useless.

Above all, individual solutions to the security risks introduced by BlackBerry will need to be configured on a case-by-case basis. While the units should not be blindly implemented without considering the data they are accessing, many of their specific vulnerabilities can be corrected. ■

## References


1. "New Attack Intercepts Wireless Net Messages," *EWeek*, March 11, 2002.
2. "AFCA Evaluation Report: Research in Motion's BlackBerry Handheld Secure Wireless E-mail Solution," *Air Force Communications Agency Communications Systems Evaluation Branch*, May 2, 2001.

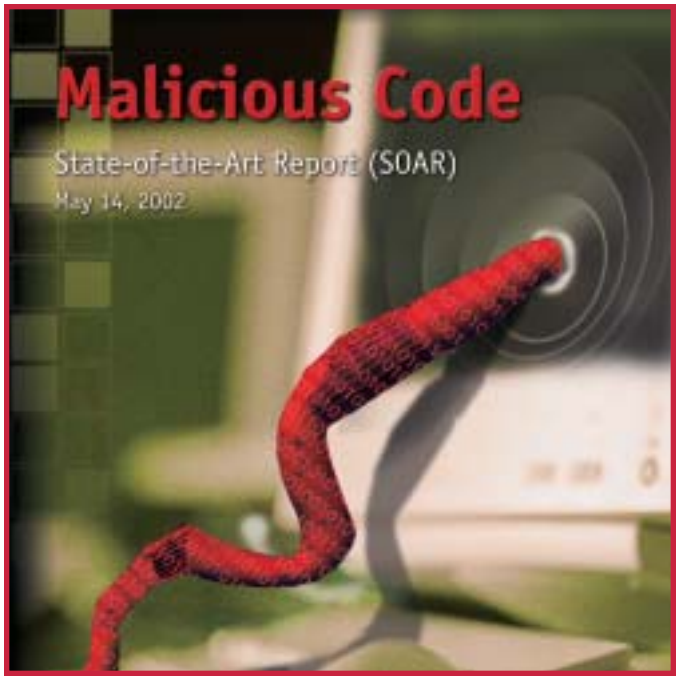

## About the Author


**Chad Tilbury**

Special Agent Tilbury is a computer crime investigator with the Air Force Office of Special Investigations. He is responsible for computer investigations and operations for Southern California. Chad graduated from the U.S. Air Force Academy with a B.S. in Computer Science and holds a M.S. in Computer Science from Northeastern University. Special Agent Tilbury can be reached at Chad.Tilbury@ogn.af.mil.



*Chad would like to personally thank the Los Angeles AFB Network Administration team, including Paul Vanderhoof, Scott Waid, and Al Basiulis for their assistance in writing this paper. Their real world knowledge and experience working with these issues was a tremendous help.*




# Malicious Code SOAR

*This SOAR updates earlier reports to DoD on the subject of malicious code, describes common detection, and prevention techniques, and provides pointers to resources for enhancing organizational information security.*

This update was considered necessary because, over the past three years, there have been numerous malicious code incidents spread through E-mail and the Internet, including several—such as the Melissa, ILOVEYOU, CodeRed, and NIMDA viruses—that caused major damage to both public and private sector information systems.

## Objective

This SOAR addresses the current state-of-the-art in detecting and responding to malicious software—"malware." The intended audience is DoD technical managers responsible for the protection of computer resources potentially susceptible to the malicious code threat. An overview of malicious code is provided as well for those that require some technical background on this topic. This report is intended to serve three purposes—

- Educate readers regarding the nature of malicious code and current trends to enhance their understanding of the threat to the confidentiality, integrity, and availability of computer-based mission-critical systems.
- Provide a framework for malicious code countermeasures as a roadmap to guide the development of strategies to combat malicious code.
- Give an overview of current COTS anti-malware products and vendors.

## Approach

The first malicious code SOAR devoted considerable attention to the evaluation of anti-virus software packages offered by commercial vendors, which were the principal controls available to combat malicious code at that time. Although the availability and capabilities of anti-virus software were limited, the threat was also relatively limited. Given the new threat environment and new countermeasures techniques and capabilities, this SOAR takes a holistic view of available methods, policies, and tools that complement the use of anti-virus software packages to comprehensively combat malicious code. The malicious code threat is neither unitary nor monolithic. Accordingly, a combination of defensive measures and techniques must be used to create a defense-in-depth without degrading the performance of operational systems to unacceptable levels.

## Scope

The danger presented today by malicious code to our nation's computer-based, mission-critical systems is greater than ever. The number of malicious code incidents continues to climb and, in several well-publicized instances, the impact on commercial information technology (IT) infrastructures has been substantial. This report uses available data regarding public domain malicious software activities to describe the threat environment and recommend and describe defensive measures. This report presents specific defensive techniques to combat malicious code. The benefit of discussing this diverse set of techniques is that it provides an additional perspective of malicious software, while at the same time providing pragmatic examples of how to defend DoD computer resources. No attempt was made to gather classified information on this subject. ■

# product 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 On-line:** http://www.dtic.mil/dtic/regprocess.html.
The *IAnewsletter* is **UNLIMITED DISTRIBUTION** and may be requested directly from IATAC.

Name _____ DTIC User Code _____

Organization _____ Ofc. Symbol _____

Address _____ Phone _____

_____ E-mail _____

_____ Fax _____

Please check one: ❑ USA ❑ USMC ❑ USN ❑ USAF ❑ Command
❑ Industry ❑ University ❑ DoD ❑ Gov't ❑ Other

Please list the Government Program(s)/Project(s) that the product(s) will be used to support: _____

_____

## LIMITED DISTRIBUTION

IA Collection Acquisitions CD–ROM

❑ Summer 2002 ed.

IA Tools Report

❑ Firewalls (3rd ed.) ❑ Intrusion Detection (3rd ed.) ❑ Vulnerability Analysis (2nd ed.)

Critical Review and Technology Assessment (CR/TA) Reports

❑ Biometrics ❑ Computer Forensics* (soft copy only) ❑ Defense in Depth ❑ Data Mining
❑ IA Metrics ❑ Configuration Management ❑ Exploring Biotechnology
❑ Network Centric Warfare

State-of-the-Art Reports (SOARs)

❑ Data Embedding for IA (soft copy only) ❑ IO/IA Visualization Technologies
❑ Modeling & Simulation for IA ❑ Malicious Code

* You MUST supply your DTIC user code before these reports will be shipped to you.

## UNLIMITED DISTRIBUTION

IAnewsletters (Limited number of back issues available)

| | | | | |
|---|---|---|---|---|
| Volumes 1 | ❑ No. 1 | ❑ No. 2 | ❑ No. 3 | |
| Volumes 2 | ❑ No. 1 | ❑ No. 2 (soft copy only) | ❑ No. 3 | ❑ No. 4 |
| Volumes 3 | ❑ No. 1 | ❑ No. 2 | ❑ No. 3 (soft copy only) | ❑ No. 4 (soft copy only) |
| Volumes 4 | ❑ No. 1 (soft copy only) | ❑ No. 2 | ❑ No. 3 | ❑ No. 4 |
| Volumes 5 | ❑ No. 1 | ❑ No. 2 | | |

Fax completed form to IATAC at 703.289.5467

## August

**2002 USSOUTHCOM Information Assurance Conference**
August 5–9, 2002
Embassy Suites Hotel, Fort Lauderdale, FL
http://www.fbcinc.com/southcomia/index.html

**CERT Conference**
August 6–9, 2002
The Peter Kiewit Institute, Omaha, NE
http://www2.cio.com/events/viewevent.cfm?EVENT=5331

**Network Security Conference**
August 12–14, 2002
Caesars Palace, Las Vegas, NV
http://www2.cio.com/events/viewevent.cfm?EVENT=5083

## September

**InfowarCon 2002, "Homeland Defense & Cyber Terrorism"**
September 3–6, 2002
Washington DC
http://www.interpactinc.com/infowarcon.html

**AFCEA Symposium "Enabling the Warfighter's Network"**
September 9–13, 2002
Fort Monmouth, NJ

**Fort Monmouth "2002 Homeland Security and National Defense Symposium"**
September 9–13, 2002
Atlantic City, NJ
http://www.afcea-ftmonmouth.org/

**Guidance Software Computer & Enterprise Investigations Conference**
September 16–17, 2002
Westfields Marriott, Chantilly, VA
http://www2.cio.com/events/viewevent.cfm?EVENT=5479

**Internet Crime Symposium: Cyber Sabotage**
September 17–18, 2002
Westin Hotel, Ottawa, Canada
http://www2.cio.com/events/viewevent.cfm?EVENT=5393

**SecureWorld Expo**
September 17–18, 2002
Meydenbuaer Center, Seattle WA
http://www2.cio.com/events/viewevent.cfm?EVENT=5381

**FIWC IO Conference (Association of Old Crows Event)**
September 25–26, 2002
Norfolk, VA
http://www.aoc.org

## October

**HTCIA International Conference & Expo**
October 1–3, 2002
Atlantic City, NJ
http://www.htcia2002.org/

**Knowledge Management Conference**
October 25, 2002
Ronald Reagan International Trade Center, Washington, DC

**MILCOM 2002**
October 7–10, 2002
The Disneyland Resort, Anaheim, CA
http://www.milcom.org/2002/

**SANS Network Security 2002 NS2002**
October 18–25, 2002
Washington Convention Center and Renaissance Hotel, Washington DC
http://www.sans.org/NS2002/

**Federal IA Conference (FIAC)**
October 29–31, 2002
The Inn and Conference Center, University of Maryland, College Park, MD
http://www.fbcinc.com/fiac/

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church, VA 22042

To change, add, or delete your mailing or E-mail address (soft-copy receipt), please contact us at the address above or call us at 703/289-5454, fax us at: 703/289-5467, or send us a mesage at: iatac@dtic.mil