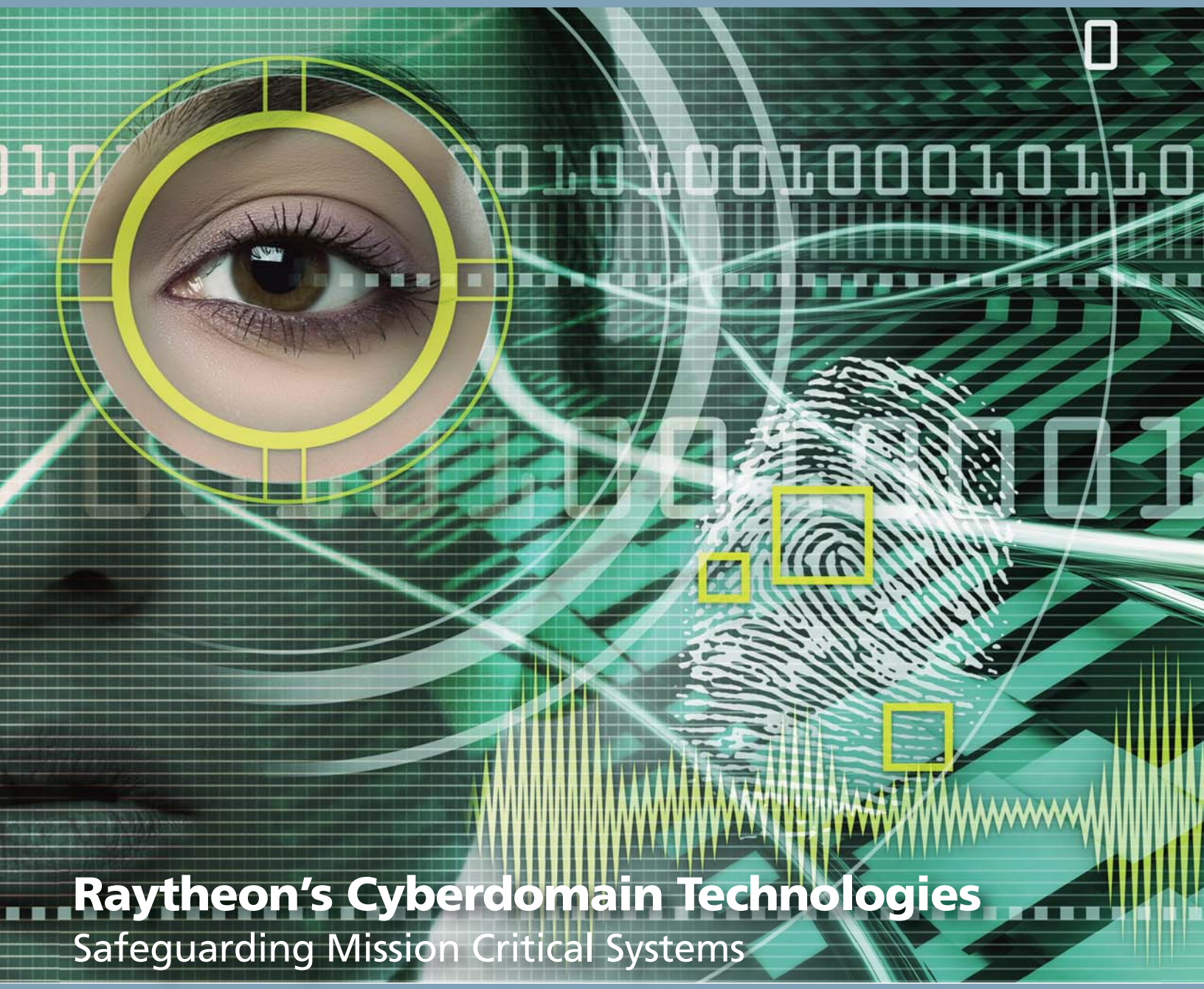
Technology Today

HIGHLIGHTING RAYTHEON'S TECHNOLOGY

2010 ISSUE 1



Raytheon's Cyberdomain Technologies

Safeguarding Mission Critical Systems

Raytheon

Customer Success Is Our Mission

A Message From Mark E. Russell

Vice President of Engineering, Technology and Mission Assurance

Cyberspace is clearly its own domain now, on par with the domains of air, land, sea and space, and like its counterparts, the cyberdomain can be just as risky a place.

Ensuring customer success in the cyberdomain requires a robust approach to assure trusted and resilient communications infrastructure and information. Raytheon's cyberstrategy can be summed up by three tenets. First, protect our internal systems, then embed cybersecurity into Raytheon's products and systems, and finally provide cybersecurity solutions to our customers.

To fulfill our strategy, Raytheon uses an integrated and disciplined process to leverage all sources of capabilities and technology. These include program funding, contracted research and development, internal research and development, and enterprise campaigns, as well as partnerships, alliances, mergers and acquisitions.

This cyberdomain issue of "Technology Today" looks at the range of Raytheon's cybercapabilities, including the company's recent acquisitions designed to integrate new skills and expertise to help solve these challenging problems. Articles look at our information assurance and information operations technologies, and spotlight Raytheon's research partnerships with universities, research centers and small businesses.

In this issue's Leaders Corner column, we hear from Raytheon Intelligence and Information Systems President Lynn Dugle about driving growth and the opportunities in the cybersecurity market. Complementing Lynn's interview are remarks by Raytheon leaders Rebecca Rhoads and Randy Fort. Rebecca is Raytheon's chief information officer and provides insight on securing our internal systems. Randy, Raytheon's director of Programs Security, gives the customer's perspective on cybersecurity by reflecting on his recent experience as U.S. assistant secretary of state for Intelligence and Research.

Best regards,

Mark E. Russell

Do you have an idea for an article?

We are always looking for ways to connect with you — our Engineering, Technology and Mission Assurance professionals. If you have an article or an idea for an article regarding technical achievements, customer solutions, relationships, Mission Assurance, etc., send it along. If your topic aligns with a future issue of "Technology Today" or is appropriate for an online article, we will be happy to consider it and will contact you for more information.

Send your article ideas to techtodayeditor@raytheon.com.

View "Technology Today" online at:
www.raytheon.com/technology_today/current

"Technology Today" is published by the Office of Engineering, Technology and Mission Assurance.

Vice President
Mark E. Russell

Managing Editor
Lee Ann Sousa

Senior Editors
Donna Acott
Tom Georgon
Kevin J. Wynn

Art Director
Debra Graham

Web Site Design
Joe Walch IV

Publication Distribution
Dolores Priest

Contributors
Kate Emerson
Christel Kittredge
Marcilene Pribonic
Sharon Stein
Keith Sturdevant

INSIDE THIS ISSUE

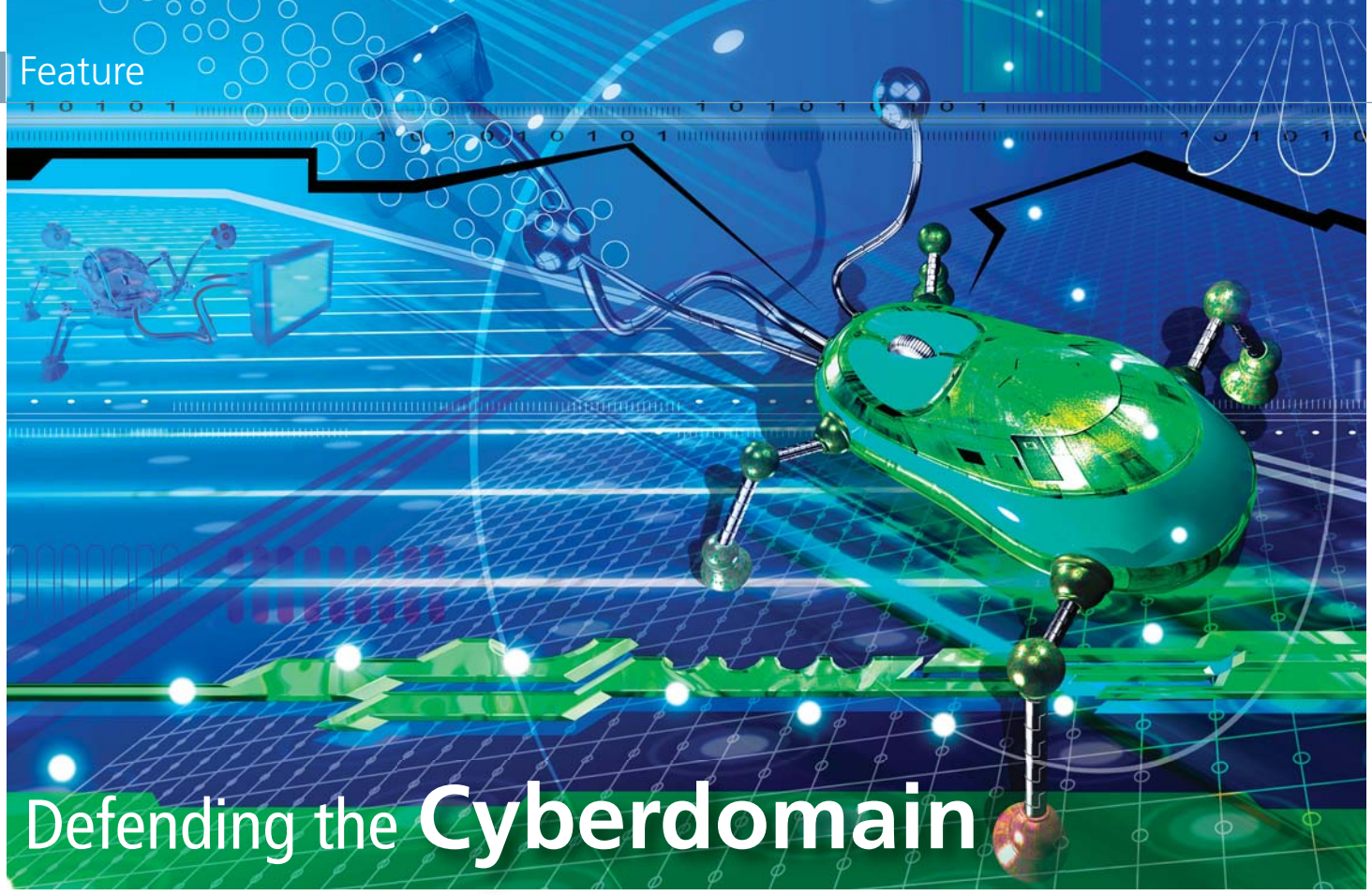
EDITOR'S NOTE

Cyberthreats, both foreign and domestic, have become a significant challenge for the world today in both military and commercial sectors. These threats can range from stealing someone's identity, to stealing company records or military secrets, to sabotaging government computers and key elements of national infrastructures. This issue addresses some of these types of threats and how Raytheon is bringing its long history of innovative technologies together in new ways to create a safer cyberenvironment for our company and our customers.

In this issue, you'll read two Raytheon leaders' perspectives on what it takes to stay ahead of the constant barrage of cyberthreats that we face everyday, as well as the customer's perspective on the cyberdomain. You'll also read about the RedWolf product line of audio and electronic surveillance systems used by such agencies as the FBI and Drug Enforcement Agency, and learn more about Raytheon's Product Data Management system — a business solution with common processes and tools that enable effective and efficient management and sharing of product information.

Enjoy!

Lee Ann Sousa



Defending the Cyberdomain

This issue of "Technology Today" is about the cyberdomain and the technologies employed to protect and respond to attacks against information and computing systems. The struggle is ongoing.

Defense Secretary Robert Gates said in a CBS News interview last year that the U.S. is "under cyberattack virtually all the time, every day." The Department of Homeland Security reported an 800 percent increase in cyberattacks from 2005 through 2007. Others estimate that in 2008, the U.S. lost $1 trillion in intellectual property, one byte at a time. Referring to cyberattacks, Air Force Gen. Kevin P. Chilton, the commander of U.S. Strategic Command, told reporters on May 7, 2009, "The Law of Armed Conflict will apply to this domain."[1]

As the country is organizing to better operate in cyberspace, Raytheon is there. Raytheon brings a history of technological innovations to the battlefield because computing systems and critical information are part of every weapon system, sensor, communications network, and command and control center it develops. Raytheon also continues to assemble the best technical talent in the world of information operations and assurance, and invests to integrate its talent and technologies.

Definitions

Information operations (IO) encompasses the technologies and techniques to affect and defend information. In the broadest sense, IO includes everything from leafleting campaigns to electronic warfare technology. But this issue of "Technology Today" is about the part of IO known as computer network operations — the ability to control cyberspace — and the thread common to the stream of troubling headlines. Although it's typical to talk about the defensive side of computer network operations (information assurance) as distinct from the offensive (computer network attack and exploitation), it's not practical to think about one without the other. A person designing a secure system had better understand how an adversary would attack it. And someone trying to infiltrate an adversary's system must protect his exploit from detection and secure its communication. Many technologies are neither inherently offensive nor defensive: What would you call a software process designed to monitor a computer's operation, respond to interesting events, and run without detection? A good anti-virus program or spyware?

As with traditional warfare, operations in the cyberdomain need to integrate and orchestrate many assets: forward-deployed sensors detect potential threats; analytics process the information to characterize an attack (Who is attacking? What are their objectives?); and proactive measures neutralize the threat before it reaches the target. Operations in the cyberdomain share some challenges with less traditional irregular or asymmetric warfare, like how to attribute threats to specific adversaries, or predicting consequences when we can wield overwhelming force. This issue emphasizes the defensive applications and an array of techniques to bring command and control to cyberspace, as well as our own strategy for cyberdomain technology.

Raytheon's approach begins with its customers, and with the recognition that they view cyberspace from different perspectives.

The first article discusses these differences, reveals what is common, and talks about operational needs and technology gaps, using techniques from the Raytheon Enterprise Architecture Process. Because the concept of fighting in cyberspace is new to many customers, Raytheon works closely with them to anticipate their needs. This element of our technology strategy is reflected in several articles about Raytheon cybertechnology in use, what we've learned as our customers' needs are evolving, and what we are doing to meet them.

The cybermarket is broad and the technology challenges numerous, and we must reach out beyond Raytheon to address them. In this issue, we look at some recent Raytheon acquisitions — unique small companies employing the best and brightest that add to our cybercapabilities.

Raytheon will always value innovation. Through many types of research and development funding we continue to invest in strategic technology. In this issue, we address several innovations coming out of our R&D efforts.

There's a lot of innovation going on in universities and small businesses. Raytheon actively sponsors advances in cybertechnology by directing basic academic research: endorsing promising small businesses as they pursue Small Business Innovation Research grant opportunities, building cooperative research and development agreements with national labs, and joining government-industry exercises. Our articles on partnerships describe where we are helping to transition emerging technologies, or where universities are helping us improve our own. ●

Jon Goding
jgoding@raytheon.com

[1] Jeff Schogol, "Official: No options 'off the table' for U.S. response to cyber attacks," Stars and Stripes, Mideast Edition, May 8, 2009.

Understanding IO Through Architecture

Enterprise architecture provides an effective set of tools and techniques for understanding customer needs and identifying applicable technologies. Raytheon's Information Operations Reference Architecture (IORA) provides a framework that can be used by business development and engineering organizations to help improve the quality and productivity of strategic analysis and design for programs and pursuits in the information operations (IO) domain. The IORA facilitates internal and external communications by establishing a common language for IO, provides a set of custom artifacts to enable strategic analysis, and enhances operational understanding through scenarios and concepts of operations (CONOPS).

What Is Information Operations?

In general, terms like "IO" or "IA" can be quite ambiguous. While most people will agree that these initials stand for *Information Operations* and *Information Assurance*, there are many differing views on the specific capabilities of each. Even customers use different vocabularies when they talk about these domains.

As a step toward enabling better communications, the IORA includes an operational capability taxonomy that establishes a common vocabulary for IO within Raytheon.

The top level of the taxonomy is illustrated in Figure 1. The focus of this edition of "Technology Today" is on the cyberdomain, but IO is even broader: It is the integrated employment of the capabilities of influence operations, electronic warfare and computer network operations.

- *Influence operations (IFO)* are focused on affecting the perceptions and behaviors of leaders, groups or entire populations.
- *Electronic warfare (EW)* refers to any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the adversary.
- *Computer network operations (CNO)* are the cybercomponent of IO and are concerned with the integrated planning, employment and assessment of capabilities to attack, deceive, degrade, disrupt, deny, exploit and defend electronic information and infrastructure.

So if IO is the entire domain (IFO, EW and CNO), where does IA fit in? IA is a subset of CNO concerned with the defense of computers and networks, and includes computer network defense and portions of network operations support, including capabilities such as assured information-sharing, cyberdomain situational awareness and shared security services.

Continued on page 6

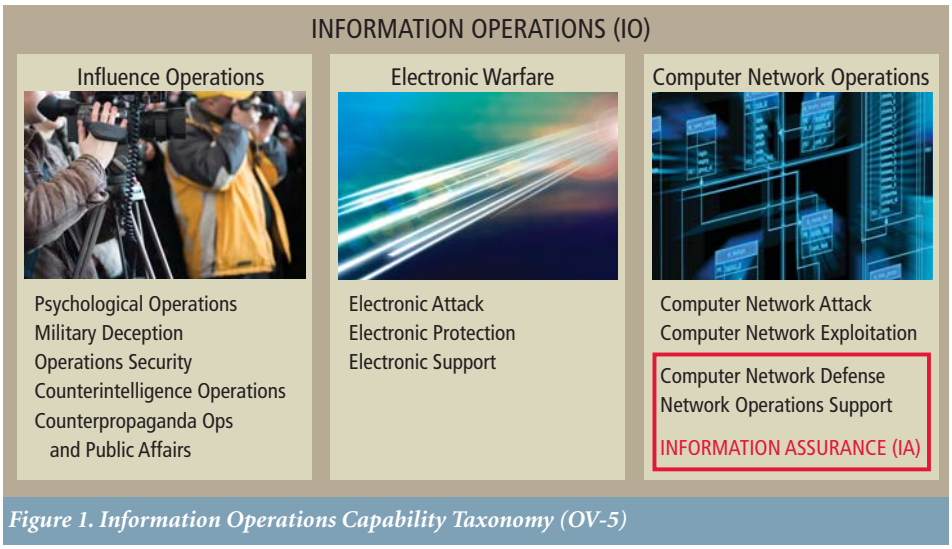


Figure 1. Information Operations Capability Taxonomy (OV-5)

Continued from page 5

It is worth noting that establishing a common vocabulary for IO is not just a matter of semantics. Differences in understanding of the basics can become a barrier to communication both internally and when communicating with customers. To address this, the IORA provides a set of translation artifacts in addition to the capability taxonomy to facilitate IO-related communications with different customer communities.

Scenarios and CONOPS

Scenarios describe the activities and events constituting a particular mission or mission segment from an operational perspective. They are useful in architecture because they help to clarify abstract customer requirements. Scenarios are typically collected in a CONOPS document that helps bridge the gap between a customer's operational needs and vision, and a system developer's technical specifications. In developing the IORA, Raytheon conducted a series of scenario workshops that provided insights into developing a CONOPS and helped highlight differences in perspectives between U.S. Department of Defense customers and intelligence community customers regarding IO. Figure 2 summarizes differences in how the DoD and IC approach their operations.

Raytheon's customers have made it clear that they want to integrate IO with other, more traditional, kinetic military capabilities. This is sometimes referred to as full spectrum operations. Recognizing this desire, the IORA CONOPS begins with a broad focus on IO doctrine, organizational relationships and planning processes. Later sections of the CONOPS take a sharper focus on offensive operations and associated scenarios.

Using the Hierarchical Threat Catalog

Raytheon has defined a new artifact, the threat catalog hierarchy, used to derive a specific architecture from a more generic, or reference, architecture. The threat hierarchy objects are mapped to architecture components such as operational activities, system functions, capabilities and services using matrices.

For selecting offensive architecture components, the mappings allow for identification of architecture components or exploits that generate the threat. For selection of defensive architecture components, the mappings allow identification of techniques to mitigate threats. Filtering for the important vulnerabilities or perceived threats quickly yields a targeted set of reference architecture components that form the basis of the implementation architecture, thus ensuring a more efficient and cost-effective solution. As the customer threat landscape evolves, the components for a technology refresh can quickly be identified based on the new filtering criteria.

Architecture as Strategy

The IORA's Strategic Architecture provides a framework for making strategic decisions in the IO domain. As illustrated in Figure 3, it provides a set of interrelated architectural views that address basic strategic questions.

Standard DoD Architecture Framework views did not provide the information needed to answer several strategic questions identified during architecture visioning (e.g., What do our customers need? What are our strengths and gaps?), so Raytheon developed a set of custom extended views for the IORA.

The IORA addresses customer needs in the IO domain using the operational capability taxonomy discussed earlier. It provides a hierarchical representation of the capabilities needed to "do" information operations.

	Department of Defense	Intelligence Community
Standardization	Standardization to achieve consistent results	Avoid standardization and predictability
Agency Cultures	Clearly defined relationships and doctrine	Relationships not clearly defined
Policy Constraints	Authority USC Title 10 Law of Armed Conflict	Authority USC Title 50 Foreign Intelligence Surveillance Act
Acquisition Approach	Mission Systems Integrator approach Systems are retained and evolve	Separate component providers/integrators Capabilities tailored for specific missions
Planning	Employs the Joint Planning Process	Creation of custom CNO capabilities Modeling of effects to obtain authorization
Infrastructure	Net-centric GIG Integrated core/tactical infrastructure	Ops infrastructure is transitory Core separate from ops infrastructure

Figure 2. Differences in Military and Intelligence Communities' Perspectives

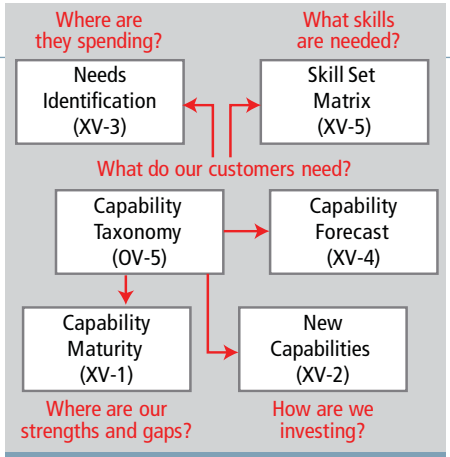


Figure 3. IORA Strategic Architecture

This taxonomy also provides a common organizational structure for many of the other artifacts within the IORA. This structure establishes well-defined relationships between artifacts and provides a more consistent framework for strategic analysis than would be provided by a collection of disconnected views.

The Operational Capability Forecast (XV-4) addresses the evolution of customer needs over time. It intentionally focuses on capabilities needed for IO versus the technologies needed to implement those capabilities.

The Market Characterization Diagram (XV-3) addresses the issue of where our customers are spending. The XV-3 partitions the information operations market (specifically CNO) into high-level categories as defined by the capability taxonomy and forecasts spending trends over time.

The Capability Maturity Matrix (XV-1) documents the capabilities of Raytheon and its competitors in various aspects of information operations. This view can be used to organize technology and identify and analyze strengths and gaps in capability across the Raytheon businesses.

The Capability Investment Diagram (XV-2) summarizes Raytheon's corporate and business investments in information operations and illustrates how those investments are distributed among the capabilities needed to provide IO solutions.

The Skill Set Matrix (XV-5) identifies the skill sets needed to design, develop, implement, and deploy IO solutions. This is useful in identifying the types of people Raytheon needs to hire or develop to provide IO solutions. ●

Chris Francis
chris_s_francis@raytheon.com
Contributors: Suzanne Hassell, Chris Cole, Jay Wiler

U.S. Air Force Cyberoperations

"Warfighters rely upon cyberspace to command and control forces in the 21st century. Revolutionary technology has presented cybercapabilities, which can provide decisive effects traditionally achieved only through kinetic means … Mastery of cyberspace is essential to America's national security. Controlling cyberspace is the prerequisite to effective operations across all strategic and operational domains — securing freedom from attack and freedom to attack. We will develop and implement plans for maturing and expanding cyberspace operations as an Air Force core competency. We will provide decision makers flexible options to deter, deny, disrupt, deceive, dissuade and defeat adversaries through a variety of destructive and non-destructive, and lethal and non-lethal means. Finally, we will do this in friendly cooperation with our professional partners and teammates in other MAJCOMs, Services, COCOMs and U.S. government agencies."

- Maj. Gen. William T. Lord, U.S. Air Force Cyber Command Strategic Vision, Feb. 2008

History — Getting to Cyberspace

The U.S. Air Force has long recognized the electromagnetic spectrum as a domain for warfare. As early as 1942, the U.S. Army Air Corps made use of radar, remotely piloted aircraft, and radio intercept and jamming. The U.S. Air Force's roots go back to the Army Signal Corps, which purchased the very first airplanes for observation. Continuing its leadership in new technologies, the Air Force was the first U.S. government organization to field a network intrusion detection device to help defend its networks at the enterprise level.

Since the reorganization of the Air Force in 1992 dissolved the AF Communications Command, Air Force cyberoperations have grown through various independent efforts. Each major command (MAJCOM) took its own path and created its own policies and procedures for maintaining infrastructure to support communications requirements. As computer networks grew in size, complexity and importance for day-to-day operations, the disparate infrastructures became unwieldy and too costly to manage. MAJCOM networks were managed independently, but were interconnected, causing risks to be shared across MAJCOMs.

In 2004, in an effort to instill common standards and streamline operations, the Air Force created AF Network Operations (AFNETOPS) within the 8th Air Force at Barksdale Air Force Base, La. The 8AF commander also became the AFNETOPS commander and became responsible for securing the AF Global Information Grid (GIG). The Air Force created the AF Network Operations Center (AFNOC) to provide command and control across the AF GIG.

Since creating AFNETOPS and the AFNOC, the advanced persistent threat to the networks has grown, and it became clear that maintaining secure networks would be essential to conducting warfare as well as day-to-day business. It was also clear that an advanced adversary would rely on computer networks as much as the U.S. The ability to disrupt or exploit those networks would be essential in conducting warfare.

In 2006, the Air Force began a more focused effort to establish a warfighting entity responsible for cyberspace operations. This organization began by designating 8AF as AF Cyber Command, responsible for conducting warfighting operations in and through cyberspace. At the same time, Air Force leadership considered various reorganization options, and in October 2008 established a new Component Numbered Air Force (C-NAF), the 24th Air Force, which would be responsible for conducting cyberoperations. The 24AF would be assigned to the Air Force Space Command as the MAJCOM responsible for organizing, training and equipping forces for space and cyberspace operations.

Continued on page 8

Continued from page 7

Cyberspace Operations

Cyberoperations are defined as "The employment of cybercapabilities where the primary purpose is to achieve military objectives or effects in and through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid."[1] The 24AF would establish, operate, maintain, defend, exploit and attack threat networks in support of Joint Operations. This mission supports Joint Combatant Command needs assigned to U.S. Strategic Command (USSTRATCOM), as defined in the Unified Command Plan (Figure 1).

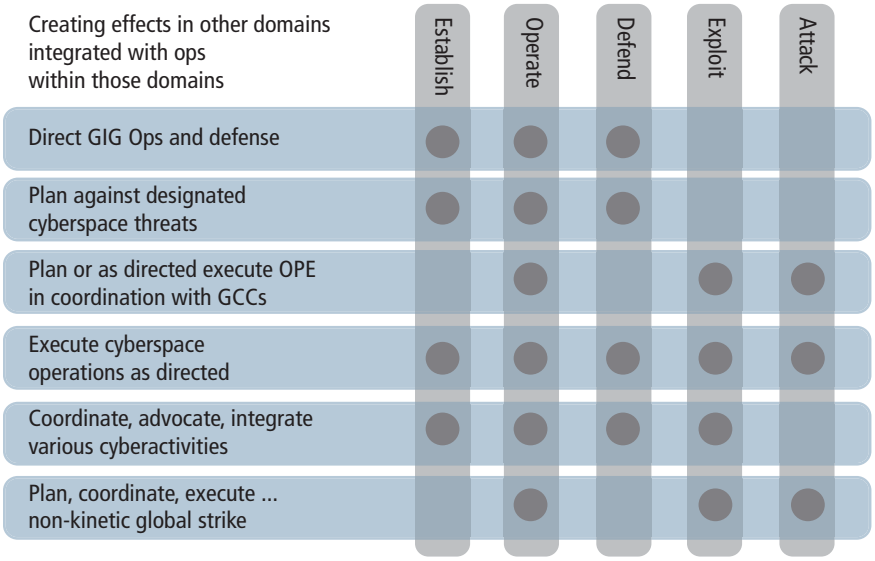


Figure 1. USSTRATCOM UCP Responsibility and AFSPC Mission Matrix

24th Air Force Organization

The 24AF will be headquartered at Lackland Air Force Base, San Antonio, Texas, where the majority of its forces are currently operating. The C-NAF will be commanded by a major general and will have a command staff of about 100 personnel. The C-NAF will operate a cyberoperations center (CyOC) that is analogous to an air operations center (AOC). The current AFNOC will grow into the CyOC, which will be organized similarly to an AOC with five divisions: Intelligence, Surveillance and Reconnaissance; Strategy; Plans; Operations; and a Cyber Coordination Cell. The CyOC will "establish, plan, direct, coordinate, assess, command and control cyberoperations and capabilities in support of Air Force and Joint Operations."[2]

The 24AF will consist of three active-duty wings with more than 5,500 personnel: 67th Network Warfare Wing, 688th Information Operations Wing, and the 689th Combat Communications Wing. The Air Force Reserve and Air National Guard will augment this force with approximately 4,500 personnel and aligned units.[3]

The 67th Network Warfare Wing is headquartered at Lackland Air Force Base, Texas, and has units spread around the world. The Wings' mission includes network operations and security, as well as offensive operations.

The 688th Information Operations Wing will be established by renaming the AF Information Operations Center (AFIOC), currently at Lackland Air Force Base, Texas. The 318th Information Operations Group and the 688th Information Operations Group, both at Lackland Air Force Base, will be aligned to the 688IOW.

The 689th Combat Communications Wing will be established at Tinker Air Force Base, Okla., and will be responsible for establishing, maintaining and defending the tactical networks necessary to support expeditionary Air Force operations. The 3rd Combat Communications Group at Tinker Air Force Base; the 5th Combat Communications Group at Robbins Air Force Base, Ga.; and the 85th Engineering and Installation Squadron at Keesler Air Force Base, Miss., will be aligned to the 689CCW.

Raytheon has committed significant resources through internal research and development projects to explore new tools for insider threat detection, malicious logic detection, network maneuverability, assurance in virtual environments, and many more. Raytheon has partnered with other companies to approach new customers, such as the Defense Cyber Crime Center, with innovative ideas in their mission areas.

Cyberoperations and Battle Damage Assessment

So what is an example of an offensive cybermission? Many examples are classified and cannot be discussed. During the Kosovo conflict, a particular telephone switch being used for command and control was identified and targeted. It was added to the air tasking order to be struck with a kinetic weapon (a bomb), but a cyberalternative was offered. The switch was taken out of service with a sort of "war dialer on steroids" that called every single extension on the switch over and over. This kept the switch constantly busy and no longer a viable command and control tool.

As non-kinetic options are developed, battle damage assessment tools must be adjusted to match the desired effect of the mission. During Operation Iraqi Freedom, a data switching center was targeted and a kinetic strike conducted. A Predator observed a big smoking hole in the roof of the building, but analysis revealed the switch was still operational. A second air strike had to be scheduled.

Establishing the 24th Air Force is just the first step in organizing the Air Force for effective cyberoperations. New cyberdoctrine is being developed and plans have been made to establish a new cyberoperations career field. The Air Force is returning to its roots to move decisively into the future. ●

[1] Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms As Amended Through March 17, 2009.

[2] 24AF Command and Control of Operations of Cyberspace Forces, May 5, 2009.

[3] HQ Air Force Program Action Directive 07-08, Change 3, Feb. 20, 2009.

ENGINEERING PROFILE

Jon Goding
Principal Engineering Fellow, Network Centric Systems

Although Jon Goding's educational background is in electrical engineering and RF communications, he embarked on a career that included large-scale computer system integration, network design and high-integrity software development.

From early on, everything Goding worked on included strict security requirements. As internetworked systems became the norm, information assurance (IA) grew in significance, and Goding applied his experience to create innovative solutions for many cross-company system design efforts and several special projects.

For the first two large projects Goding worked on in the 1980s, he faced difficult IA challenges and very high mission-availability requirements. "These weren't the kinds of skills taught in the standard electrical engineering curriculum at the time, so I had to learn on the job," he said. "I've always enjoyed working on difficult problems, and information assurance has presented me with those."

A 23-year Raytheon veteran, Goding presently serves as chief engineer for Raytheon's Information Operations campaign, where he is responsible for coordinating cross-company research and development in information operations and information assurance.

Goding served as the information assurance architect for the Navy–Marine Corps intranet from preproposal through initial operations. At the time it went operational, NMCI was the largest integrated secure network in use. When Raytheon formed a new Secure Networks product line, Jon was named its technology director.

Goding is a Raytheon Six Sigma™ Expert, and a co-inventor of several Raytheon information assurance innovations.

Raytheon High-Speed Guard

The Raytheon High-Speed Guard (RHSG) provides critical technology for sharing data between security domains. As of July 2009, Raytheon deployed 170 systems. Lead engineers for the project continuously support customers by monitoring requirements, technical challenges, and trends to ensure that customers' information-sharing and information-protection needs are met.

What Is a Guard?

Current security policies require a trusted entity to independently validate data being moved between top secret, secret, releasable and unclassified networks. These products are commonly known as trusted guards, high assurance guards, or just guards. Guards typically function as proxies, providing network separation between the two systems being connected. A guard has three main functions:

- Network separation
- Mandatory access control
- Data validation

Network Separation

A guard separates networks by providing an IP address on the high-side network as well as one on the low-side network. This allows the guard to appear as an end node — a server — on each network without making one network visible to the other. A guard specifically does not pass routing information, dynamic host configuration protocol (DHCP) requests, or other control-plane information from one network to the other. Guards provide proxy network connections and restrict the flow of network traffic to a constrained set of IP addresses, ports and protocols.

Mandatory Access Control

Another requirement for guards is to enforce mandatory access control. MAC is one of the most enduring concepts in information assurance. In a nutshell, MAC describes the requirements for ensuring that every action is identifiable with one or more actors (users, applications or systems), and that the information acted upon is dominated by the privileges of those actors. Ensuring these simple criteria are met — even in the face of programming errors and malicious users — typically requires a trusted operating system such as Security Enhanced Linux®. In a trusted operating system, the operating system carries label information on all components on the system: memory, file systems, network interfaces, etc., and provides application programming interfaces for systems such as guards to move data between security levels.

Data Validation

A guard must validate the data passing through it and ensure the data is authorized. Guards typically enforce different checks depending on the direction the data is flowing.

When data is passed from a high to low network, the guard ensures that only data authorized at the lower network's security level is passed. Several methods are used, including the following:

- Classification rules to independently interrogate the data to determine its classification
- Verification of existing labels on data
- Verification of upstream systems' digital signature on data

Continued on page 10

Continued from page 9

The right combination of methods depends on a particular system's data formats and security policies. For moving data from a lower network, the primary concern is the prevention of malicious content. For file-based transfers, virus scanning is the primary mechanism for meeting this requirement. For streaming data, data validation can be used to verify the content of the data by checking individual field values for compliance to the data specifications.

Meeting Critical Customer Needs

The need to share intelligence has become one of our critical customer requirements. Data collected at higher security levels is typically processed into intelligence meant to be shared at lower security levels, including releasable data for coalition partners. Command and control systems in the field require automated access to higher security-level tasking and reporting systems. Figure 1 shows an overview of how Raytheon's guard might fit into system architecture.

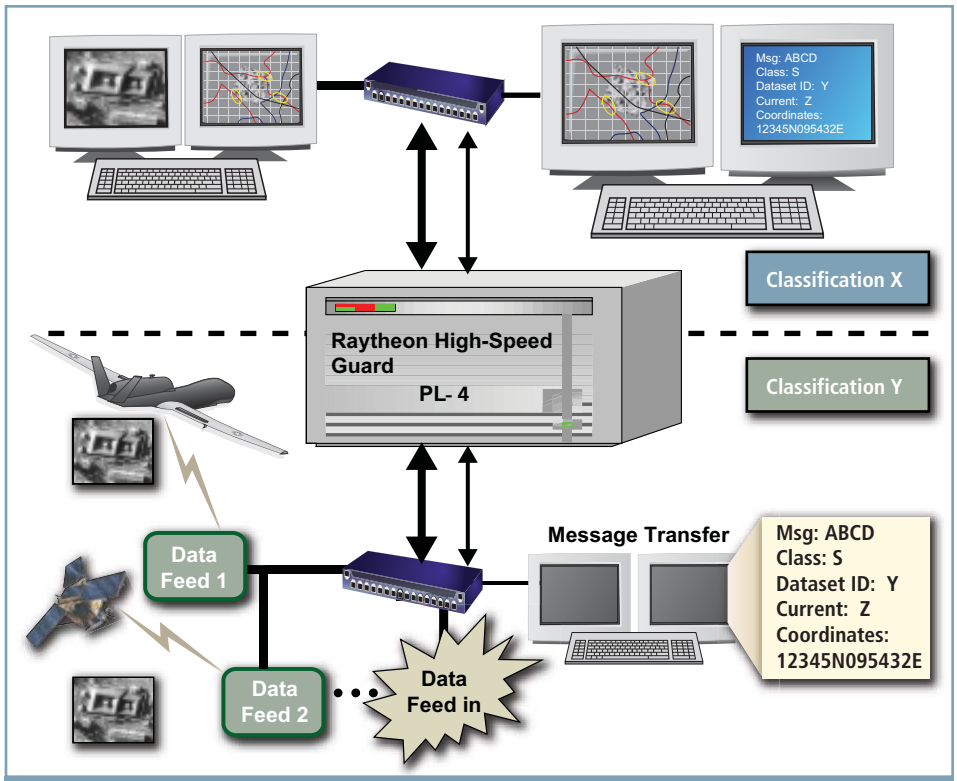


Figure 1. The Raytheon High-Speed Guard provides a high bandwidth, low latency cross domain solution for most intelligence community and DoD data types.

Current guard systems are typically limited to pre-defined, fixed-format data types. As customers adopt such current commercial approaches as service-oriented architecture, they introduce significant challenges for secure cross domain implementations. Key challenges include evolving standards and new transport protocols for guards like Standard Object Access Protocol (SOAP) over HTTP.

The RHSG team tackled these challenges in the last three years by providing the cross domain solution for the Empire Challenge intelligence, surveillance and reconnaissance (ISR) demonstrations sponsored by the Under Secretary of Defense (Intelligence). The exercise included a full range of two-way cross domain information exchange, including traditional file transfers, live streaming video and Web service transactions via SOAP messages transmitted over HTTP. During the execution of Empire Challenge, the RHSG supported hundreds of thousands of cross domain transfers.

The cross domain Web services demonstrated the first implementation of Distributed Common Ground System (DCGS) Integration Backbone federation across releasability domains, providing support for data query and product retrieval. Based on the successful demonstrations, our customers are looking to deploy this Cross Domain Federation Service in support of the warfighter.

With SOA Web service architectures becoming the standard for new systems for our customers, Raytheon was awarded one of two 12-month Proof of Concept contracts to develop the next generation of cross domain systems for another of our U.S. Department of Defense customers. The Distributed SOA-Compatible Cross Domain Service program seeks to define a cross domain system capable of supporting entire enterprises via a system of scalable cross domain services accessed as Web services.

Looking to the future, Raytheon is supporting university research on natural language processing and automatic data classification. Breakthroughs in these areas are keys to further streamlining cross-domain transfer validations in terms of cost, schedule and performance. ●

Kevin Cariker
kevin_l_cariker@raytheon.com
Jason Ostermann
josterm@raytheon.com

Raytheon's Strategy for Meeting the Cybersecurity Challenge

Pick up a newspaper on almost any day and you get a sense for the magnitude and seriousness of the cyberthreats faced by government and industry around the world. Identity theft, intellectual property theft, spam, and even the disruption of an entire country's Internet service[1] are all too common. Raytheon has long recognized the threat and the overriding national security imperative to protect our own intellectual property, as well as the critical defense information that our customers entrust to us. We therefore aim to maintain a world-class, industrial-strength cybersecurity program, embodied in our RTN Secure strategy.

Our operational strategy is to focus not only on stopping malicious inbound traffic, but also watching outbound traffic and insider threats. We are collaborating with government and industry partners to ensure the communications between our companies is also secure and our data is protected while in one another's care.

Risk-based Investment Acceleration

RTN Secure is, above all, a risk-based strategy. We continuously evaluate all of the risks we face in order to prioritize our investments against the highest risks and highest payoff. We add to our own evaluation by seeking out expertise from a wide cross section of the security community, including our own information assurance and information operations experts and Internal Audit team, as well as third-party assessment teams. The result is a comprehensive risk assessment that has shaped more than two dozen projects since 2007.

In previous years our investments were network-focused, expanding our ability to monitor our network and take action on detected threats. It was manifested in an increase in monitoring tools and collection points, tools to correlate the information we collect, and manpower with the hard-to-find skills to make sense of the results. We've realized significant return on our investment, and we continue to invest in our network security architecture in response to new threats.

Continued on page 12

Rebecca Rhoads on Cyberscurity Strategy

"Raytheon is a global technology and innovation leader where security is an overarching requirement, and information assurance is an ongoing responsibility for every employee.

Yes, cyberattacks are increasing every day — but our innovative cybersecurity strategy is strengthening our competitive position, and protecting us while ensuring success for our customers."

Rebecca R. Rhoads
Vice President and CIO
Raytheon Company

Continued from page 11

Our primary effort in 2009 was our Workplace Management Initiative, which is designed to extend our security improvements down to the desktop through an initial rollout of the RTN Secure Computer based on the Windows Vista® operating system as a precursor to widespread rollout on Windows 7® beginning in 2010. At its core, the initiative has two goals. The first is to reduce the variability of desktop and laptop operating system images within the company. This will reduce our IT support costs, and more importantly, it will result in a more consistent and predictable environment to defend and monitor. The more variability there is in the network, the more difficult it is to distinguish between malicious and normal activity. The second, closely related, goal is to provide a secure, managed common operating environment for our employees through standardized and strictly enforced desktop security configurations modeled after the Federal Desktop Core Configuration. We have put in place extensive background procedures and capabilities to ensure the more secure desktop still provides our employees the flexibility to get their jobs done safely.

Another multi-year effort that is coming to fruition is our public key infrastructure (PKI) implementation. This is a collaborative effort with the U.S. Department of Defense (DoD), other major defense contractors, and the CertiPath PKI bridge to build a trusted identity and encryption environment. This will allow us to log into DoD Web sites using our own employee credentials and exchange encrypted e-mails and documents with our customers and peers. Internally, PKI will also enable us to move toward two-factor authentication using a USB token, which will be a major step forward in preventing an attacker from using stolen passwords.

Collaboration

In some ways the problem of defending the cyberdomain is no different from the problem of defending our nation's airspace. The U.S. military and our allies must all operate in the same airspace and face the same airborne threats. We've long recognized that victory in this environment can only be achieved if we are all exchanging threat information, coordinating and de-conflicting our efforts, and operating in a common command and control environment.

The cyberdomain is much the same. We are all operating on the same cyberbattlefield and seeing the same threat. By pooling our threat information, reacting in a coordinated manner wherever possible, and operating from a common view of the battlespace, we are more successful collectively than we could ever be individually. Raytheon, therefore, has made collaboration with government, industry, and even our own employees a centerpiece of the RTN Secure strategy.

Our flagship collaboration effort is through the Defense Industrial Base (DIB) Cyber Security Pilot Program. In this cooperative effort between the DoD and more than two dozen cleared defense contractors, DoD serves as a clearinghouse for disseminating threat information received from all participants and adds additional classified threat and background information. Raytheon has significantly raised our security posture through this partnership, and we share threat information we have obtained through our own monitoring and investigative efforts.

We complement our DIB collaboration through membership in the Defense Security Information Exchange (DSIE). This is an industry-only forum chartered under the Department of Homeland Security's Critical Infrastructure Protection program. Where the DIB often operates at the classified strategic level, the DSIE is focused on real-time collaboration between technical analysts. The DSIE is setting new standards for open sharing of sensitive attack information because the charter is set up to isolate the DSIE effort from any business competition between companies. Because of this independence and the speed of the collaboration, we are often able to quickly detect and thwart attacks that span multiple companies.

We have also recognized that we must work with our customers and business partners to create an interoperable, secure collaboration environment for day-to-day business. To that end, Raytheon is a founding member and governance board leader of the Transglobal Secure Collaboration Program. Through TSCP, we develop common procedures and technical standards to securely exchange information across national boundaries and companies.

Raytheon Oakley Systems and Raytheon SI Government Solutions — two recent Raytheon acquisitions — provide us with additional opportunities for enterprisewide collaboration. These new additions to the Raytheon team allow us to tap a new source of products and expertise. Raytheon can also provide these organizations with additional expertise in cybersecurity, as well a large network test bed to ensure that products are rock-solid before they are delivered to our customers.

But for all the collaboration and information-sharing efforts, our most important relationship is the one we establish with our employees through our security awareness campaign. For all our technologies, our people are our last and best line of defense, because alert and educated employees do not fall victim to socially engineered attacks. We know our continuing awareness campaign is working simply by the number of suspicious e-mails our employees report to us and the decreasing number of people who are opening those e-mails.

Operational Acceleration

Operationally, Raytheon is balancing our secure services with a strategy that expands defensive actions to detect, disrupt and deny attackers' communications back out to the network. This strategy is based on the premise that if attackers get into your network but cannot communicate back out, the attack is effectively thwarted. Such a strategy focuses on detecting and blocking the Web sites, covert channels, and IP addresses used by attackers.

A focus on the outbound traffic has the added benefit of decoupling our detection capability from the attack vector. Attack methods change often, but attacker command and control techniques tend to vary much less frequently and are independent of the original attack mechanism. Thus, without losing sight of the need to close new vulnerabilities, we are able to operate at a more consistent operational tempo.

This strategy is made possible by our infrastructure and collaboration investments. It relies heavily on traffic analysis, both automated and manual, to sort through our logs and network routing patterns. It leverages the new network monitoring capability we installed through RTN Secure. To facilitate this strategy we reengineered portions of our network to channel risky traffic to known routes. Along with our Workplace Management Initiative, this greatly improves the signal-to-noise ratio on our network, making traffic analysis much more effective. The strategy also relies on our collaboration efforts. We identify a significant number of command and control channels via our own efforts, and we also leverage the efforts of our collaboration partners.

Industrial-Strength Cybersecurity

Every day in Raytheon we face the challenge of defending against threats in a very large and diverse enterprise. With RTN Secure as a long-term strategy, we are confident we can continue to protect Raytheon's network, our employees' privacy, and our company's and nation's critical information. ●

Jeff Brown
jeffrey_c_brown@raytheon.com

[1]Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," Wired Magazine, August 2007. http://www.wired.com/politics/security/magazine/15-09/ff_estonia.

ENGINEERING PROFILE

J.C. "Jay" Smart
Chief Technology Officer, Intelligence and Information Systems

While an electrical engineering student at Northwestern University, Jay Smart headed west on a motorcycle to begin a career that would lead him to Lawrence Livermore National Laboratory. From his first official work assignment 30 years ago — designing an apparatus to measure the approximate yield of an underground thermonuclear detonation — to his current role as chief technology officer at Raytheon Intelligence and Information Systems (IIS), Smart has dedicated himself to advanced technology research.

Smart completed his Ph.D. in the early 1990s, and he thought he would never again need to refer to his dissertation, "Dependency Visualization for Complex System Understanding." However, he said, "I was wrong."

Smart recalled, "In the mid-1990s, I was visited by two men in dark suits, with U.S. government IDs." The men were looking for potential solutions to an emerging class of cybertechnology challenges. "I basically had my lunch hour to prepare, so I took my dissertation off the shelf and used it to formulate a graph-based approach to a field that has subsequently become known as information operations."

This approach led to the development of a series of automated software tools and techniques that helped launch the Information Operations, Warfare, and Assurance Center in 1996, where Smart served as the first director. Smart later served as the technical director for the National Security Operations Center, where he provided technical oversight of cryptologic mission management, before joining Raytheon in 2007.

At Raytheon IIS, Smart is responsible for managing advanced technology research and development for Raytheon customers from the intelligence, homeland defense and security communities.

Raytheon's Cybercapabilities:

Raytheon is a world-class provider of cybercapabilities. In order to maintain a robust presence in this environment of rapidly changing technologies, Raytheon acquired five firms with well-established reputations for excellence in the cyberfield:

- SI Government Solutions, which teaches us how to attack
- Houston Associates, which understands network operations on a global scale
- Oakley Systems, which is showing us how to defend
- Telemus Systems, which brings total security architecture
- BBN Technologies, which taps its research and development expertise for innovative solutions

The work of these companies highlights Raytheon's commitment to bringing comprehensive and innovative solutions to our customers.

Raytheon SI Government Solutions

In 1999, the looming threat of the Y2K bug generated renewed interest in software testing. At Florida Institute of Technology, Dr. James Whittaker, a nationally recognized thought leader in advanced software testing techniques, was creating a new paradigm and methodology that dramatically enhanced the ability to find bugs in software.

As companies vied to have their beta releases tested in Florida Tech's classrooms, the only bugs that were really noticed by the vendors' programs were the ones associated with security. This in turn drove the students to focus exclusively on security flaws. The new methodology that was emerging was a holistic view of software. It recognized that applications do not execute in isolation; rather, there is a complex interaction between the system and the applications it supports.

As part of this new direction, a need developed to "get under the hood" in order to gain the visibility necessary to reason about software in a dynamic execution environment. This meant that the standard tool set was entirely inadequate; a new set of powerful low-level system tools was required, and the students began to build them. Better tools translated to more bugs found. In fact, the students were so successful in finding bugs that the associated grants from industry funded the Center for Information Assurance at Florida Tech. These tools were so powerful that the users could literally bend software to their will.

For example, a tool was built to support expert witness testimony in a case involving a company's claim that firmware supporting RAM could be modified, causing unrecoverable damage. Specifically, the exercise demonstrated that the EEPROM (electronically erasable programmable read-only memory) single photon detector data area locked by the backside input/outputs could be overwritten. The tool successfully demonstrated that DRAM was vulnerable to unrepairable damage through software, and the company won its case.

By 2002, everyone was becoming aware of the sparks flying out of the Florida Tech Computer Sciences department. In an effort to capture this talented group of individuals, plans were made to start a company focused on application security, and in 2003 Security Innovation was formed. In 2005 SI Government Solutions spun from the parent organization with six core individuals, and within three years was making more than $14 million in sales.

Today at Raytheon SI Government Solutions, the excitement and high tempo of a start-up remain and form an integral part of its success. The company remains focused on the original methodology that has served it well in this domain. It is a methodology that forwards one of the main tenets of the cyberlandscape: Real attackers attack software to gain the keys to the kingdom.

Excellence and Acquisitions

Houston Associates

In January 2006, Raytheon acquired Houston Associates, Inc. (HAI), then a 24-year-old company focused on network operations, coalition operations and command and control capabilities. Recently, HAI was renamed NetOps and Information Solutions (NIS) and continues to be intimately involved in championing, refining and implementing the U.S. Department of Defense's (DoD) NetOps vision for mission-critical coalition networks, through the delivery of advanced situational awareness capabilities for the Global Information Grid (GIG), and through research and development.

When HAI was established in 1982, the company provided PC-based decision support information systems to municipal governments and the Department of Health and Human Services, establishing a strong record of performance and reputation in a difficult market.

During the next 15 years, the company sought to broaden its client base, management and technical depth in the federal market. The Defense Information Systems Agency (DISA), DARPA, and FEMA became new customers with contracts for the Defense Simulation Internet and many broader-based engineering, deployment, installation, and network management support programs. On DISA's Leading Edge Services contract, NIS showcased advanced capabilities, including the first operational ATM network within the DoD and the first operational implementation of ATM over satellite.

NIS has grown to more than 250 employees and began to reach into higher end software and network-centric enterprise capabilities. NIS supported many advanced concept technology demonstrations. The company also provided technical support to network-centric enterprise services research and development as well as early prototyping of the Net-Enabled Command Capability through DISA pilot programs such as NCC and Horizontal Fusion. On the NCC pilot, NIS created the first application to consume and produce Net-Centric Enterprise Services-compliant Web services.

During this period, NIS also branched out into a new area for DoD: NetOps. This growth began with an innovative network performance forensics tool called RV+ that NIS engineered for DISA. Later, this tool became the basis for DISA Network Common Operational Picture and eventually the Global Information Grid Common Operational Picture program where NIS provides cyberenterprise situational awareness and correlation and fusion capabilities for all aspects of GIG operations from information assurance and defense to help desk operations and network performance management.

Meanwhile, Defense Information Systems Network–Leading Edge Services transitioned from a research network to an operational environment and NIS pursued another emerging set of warfighter requirements in the coalition space out of Multinational Information Systems. Under MNIS, NIS is responsible for engineering and operations of the Griffin, MICWAN, CFBLNet and portions of the CENTRIXS coalition networks — 24/7/365. NIS supports MNIS in hosting the Coalition Warfighter Interoperability Demonstration, or CWID, by planning the event, organizing participants, and providing all network services for the demo in a new location every year.

The mission and concept of NetOps became the primary mission for NIS in the mid-2000s. Through existing programs, NIS leaders like Dr. Sailaja Raparla, director for NIS and also a member of the Air Force Scientific Advisory Board, became highly visible supporters with DISA, OSD, JTF-GNO

Continued on page 16

Continued from page 15

leadership, gaining public customer praise for championing the vision as a corporation. NIS produced original research and patents on various topics, including papers on end-to-end enterprise management, on multilevel precedence forwarding and others that have furthered the state of the art to include service-oriented architecture and Web service management and monitoring.

Raytheon Oakley Systems

In October 2007, Raytheon acquired Oakley Networks, Inc., an eight-year-old company focused on scalable end-point monitoring solutions for information assurance purposes. Oakley's products are used for combating insider threats ranging from counterintelligence to vendor collusion, and advanced persistent threats ranging from detection of external manipulation of insiders, to detection of forensic artifacts left behind by attackers.

Although nearly every organization has secrets it wants to protect, those secrets are so diverse that insider threat solutions need to be robust and extensible. Secrets range from customer lists to secret formulas, or even classified locations of undercover agents. The secrets can be electronic or physical, or both, and when the secrets are not digital, technology solutions need to be sensitive enough to look for digital indicators of their physical misuse. Other insider threats include violence, sexual harassment, damage or destruction of information and property, faulty business processes or decisions, and other actions that can threaten an organization's continuity and viability.

Oakley's solutions provide organizations visibility into the range of possible threats by providing a near-time policy-based monitoring framework that allows customers to look for new threats they previously had no ability to anticipate, and measure the rate and severity of those threats. Organizations need better monitoring and auditing tools. The world has moved from the analog age, where accurately judging trustworthiness was accomplished through constant face-to-face interaction, to a digital age where we're lucky if we can attempt to judge trustworthiness based on a brief glimpse of an e-mail thread; and from an analog age where right-sizing permission consisted of a big combination lock on a paper-file cabinet, to digitally prescribing which of thousands of files a user should and should not have access to.

Raytheon defines insider threat management as a continuous process of assessment, policy definition, risk mitigation, situation analysis and remediation. Raytheon SureView™ is a host-based insider risk management solution that identifies and supports investigations of user violations so that organizations can proactively manage insider incidents. Collected data is viewed in video-like, near real-time replay that displays the user's activity, including keys typed, mouse movements, documents opened or Web sites visited. With video replay, man-hours are saved by quickly determining a user's motivation and intent.

Raytheon Telemus Systems

In July 2008, Raytheon acquired Telemus Solutions. Telemus has been a consistently reliable global provider of diversified security and intelligence solutions serving a variety of U.S. and international clients that include federal, state and local government, Fortune 500 companies, utilities, and professional associations.

Telemus products and services include private and public sector consulting, research and analysis, threat and vulnerability assessments, information security, independent verification and validation, reverse

ENGINEERING PROFILE

David Wollover
Director, Raytheon Telemus Engineering

David Wollover has enjoyed more than 20 years of advancing a variety of programs for the intelligence community, Missile Defense Agency, Office of the Secretary of Defense, U.S. Air Force Center for Studies and Analyses, USAF Space and Missile Command, USAF Weapons Lab, U.S. Marine Corps Headquarters, U.S. Naval Air Systems Command, and different quasi-public laboratories.

A natural desire for learning guided Wollover through a diverse career path, from Navy aviation, to Air Force modeling and simulation, satellite and missile design and deployment, laser technology, unmanned aerial vehicles, commercial off-the-shelf integration and information operations.

"The most vital event energizing my engineering outlook occurred at Virginia Tech, where I had the distinct privilege of taking ENGR 5004, the graduate-level systems engineering course from Dr. Benjamin Blanchard," Wollover said. "This generous man reached into the interest I displayed in his course knowledge and persuaded me to revamp and power my systems thinking at scores of levels."

He continued, "A huge personal success driver was being fortunate enough to serve clients with missions that breed infectious passions. I see younger engineers facing challenges in discovering the right learning opportunities that will stretch them beyond their comfort zone. Some good advice I received long ago was don't just accept change, but become more proficient in taking charge of it. Realize the more you educate and sweat the details, then better quality choices shall become yours. As engineers we have a special privilege of shaping the future."

Wollover describes his perspective on managing client programs: "As we see client requirements become more fluid, we become more agile in focusing on our client processes in order to discover opportunities for innovation. This requires not just flexibility, but instilling among all our talented engineers an appetite for persistent learning and re-thinking 'conventional wisdom.' We strive toward everyone becoming capable of stepping up to full technical leadership in forging solutions in the fire of their aggressive intellects."

engineering, customized training, systems integration, and a variety of made-to-order information technology services.

Telemus originated as O-Tech International in 1990 to support U.S. companies operating overseas. In 2000, O-Tech merged with Security Management International and was renamed Telemus Solutions. After the events of Sept. 11, Telemus supported the priorities of counterterrorism organizations, the intelligence community, the DoD and the Department of Energy.

Telemus is primarily divided into three areas: Engineering, Research and Analysis, and Infrastructure Protection Services.

Telemus Infrastructure Protection Services delivers customized vulnerability assessments for air and sea ports, water and power utilities, natural gas systems, nuclear facilities, and private businesses. These assessments provide insight and direction to guard clients from intrusions or attacks. Telemus has developed emergency planning systems or sub-systems at the industrial, regional, state, county and municipal levels.

Telemus Research and Analysis has broad and deep expertise in open source and restricted source research for government and private sector clients. Projects include discretionary fact gathering, data collection and organization, information brokerage, in-depth intelligence review, and documented analyses and assessments. Telemus excels in source verification, analysis and forecasting.

Telemus Engineering executes in client-driven technical domains as we perfect our go-to-market capability-tailoring to a widening client spectrum. Key domains include: applied wireless technologies; device/component reverse engineering and analysis, hardware engineering, SCADA security solutions, vulnerability assessment, and penetration testing.

Raytheon BBN Technologies

In October 2009, Raytheon welcomed its newest addition, BBN Technologies — a world leader in research and development, and provider of critical solutions for national defense and security missions.

As Raytheon BBN Technologies, the organization leverages expertise spanning information security, speech and language processing, networking, distributed systems, and sensing and control systems. Through broad technology expertise and rapid development, it researches, develops, prototypes and delivers innovative solutions quickly to meet critical needs.

In the cyberdomain, Raytheon BBN Technologies conducts research, development and deployment of information security technologies and provides assured network solutions to complex operations and planning problems.

It helps protect national security interests by performing leading-edge research and development for U.S. government customers such as DARPA, NSA, DISA, and the service laboratories. Its capabilities and services include denial of service triage, designing protection and adaptation into a survivability architecture, high-speed encryption electronic board design, quantum cryptography, and security standards development. ●

Terry Gillette
tgillette@sigovs.com
J.P. Leibundguth
jpleibundguth@hai.com
Ken Davis
ken_r_davis@raytheon.com

ENGINEERING PROFILE

Matt Payne
Principal Software Engineer
Raytheon Oakley Systems

Matt Payne's interest in software began when he was a kid, with a course in LOGO programming. From that point, he said, "I kind of always knew that this is where I wanted to be."

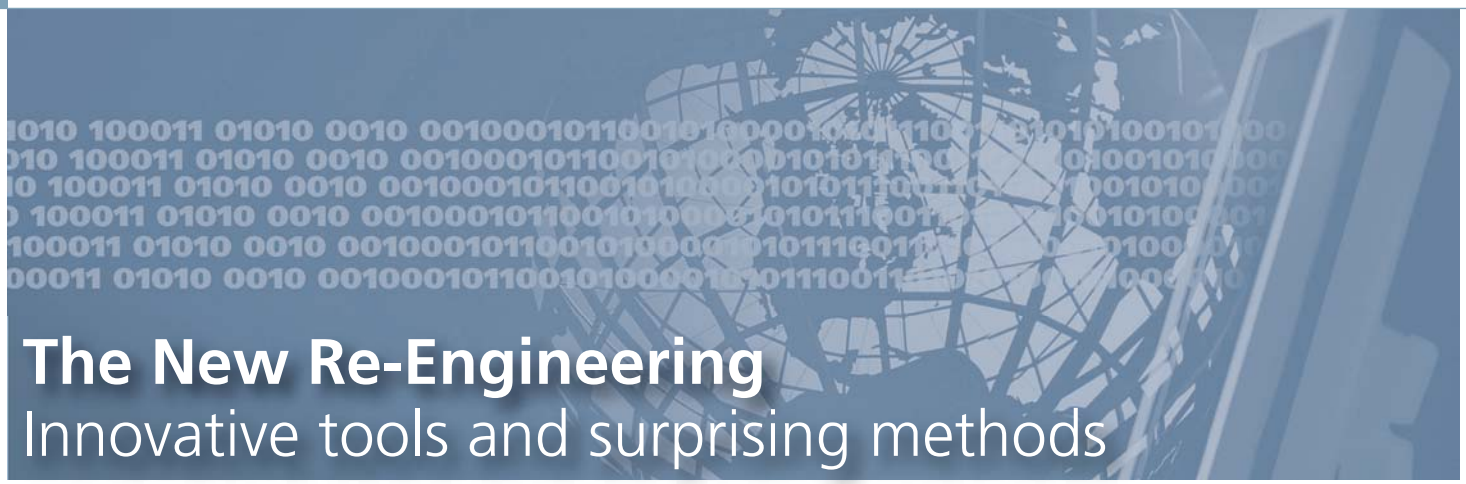
The motivation sparked then continues today in his work on the Raytheon team. "I work with a lot of really smart engineers — people with a huge amount of experience and a wealth of great ideas. That provides a lot of motivation to keep up with the talented and bright minds I'm surrounded by every day."

As a principal software engineer, Payne designs and builds software systems to support Raytheon Oakley Systems products that help protect customers' critical infrastructure and assets — both physical and human.

Payne enjoys the variety that working at Raytheon brings. "As a large organization, Raytheon provides a lot of unique opportunities to work on cool stuff and solve interesting customer problems."

During the past several months, Payne collaborated with colleagues in another Raytheon business to build a hypervisor root kit. "That has allowed me to step outside of my normal work routine and contribute my knowledge and experience to the success of a project that originated in a different part of the company."

For Payne, one of the most satisfying aspects of his job is knowing that he is supporting the warfighter. "It's great to work for a company that has a proven track record of success. When you hear about how our solutions have protected our country and kept soldiers and others out of harm's way and you know that you've played a part — there's a lot of satisfaction in that."



The New Re-Engineering
Innovative tools and surprising methods

Vulnerability research has historically been a disorganized process, with a collection of custom approaches used by different researchers with inconsistent results. Indeed, consistency is one of the most difficult aspects of vulnerability research — it's a never-ending hunt for the proverbial needle in the haystack, except a particular needle might not even exist. Despite the difficulty of the challenge, Raytheon SI Government Solutions has a track record of proactively identifying vulnerabilities for a variety of customer applications using an advanced tool set beyond the public state of the art.

Reverse engineering in the context of vulnerability research is taking apart an application to understand how it operates so that flaws in its operation may be discovered and either corrected or exploited. Whether the end result is to support an information operation mission or to improve information assurance, the process of reverse engineering to discover vulnerabilities is similar.

Current reverse engineering tools to support vulnerability research are fragmented, as are the approaches researchers use. Debuggers and disassemblers help to focus on specific narrow functionality, but are impeded by binary obfuscation and armoring mechanisms employed to protect intellectual property within software. Those mechanisms make binary analysis difficult by modifying normal instruction sequences in manners that make analysis more difficult (adding extra useless instructions, encrypting portions of code, etc.). Additionally, current reverse engineering tools are not designed to create the larger picture of a program's functionality. While decompilers that attempt to re-create source code help at abstracting to a higher layer, they are even more susceptible to problems from binary obfuscation. Additionally, those approaches don't necessarily identify vulnerabilities — they just help a reverser understand how the program functions. Other approaches, either automated or manual, must be used to actually identify potential vulnerabilities.

Industry's Cutting Edge

Current public state-of-the-art reverse engineering tools are just now beginning to make strides in the area of automation, completeness and scale.

Automation is used for multiple purposes. Some tools may attempt to automatically strip away binary protections; others may attempt to identify common vulnerability sequences. While automation can be limited, tools that feature extensible application program interfaces, scripting interfaces, or other mechanisms to easily automate common tasks are much more powerful than stand-alone tools that only operate with a human typing and clicking. One of the problems with automated source-code analysis solutions is the signal-to-noise ratio. Within an application comprising millions of lines of code, there may be thousands of errors — an error being code that contains the potential for unintended behavior — most of which cannot be exploited and offer no security risk. When attempting to identify the most critical problems, knowing which errors are exploitable (i.e., which constitute vulnerabilities) and understanding what it takes to exploit one vulnerability versus another allows resources to be most effectively allocated in securing the software.

Reverse engineering efforts to discover vulnerabilities are only as effective as the code they can touch. In fuzzing, for example, corrupted input is sent to an application to discover if it handles it properly. Effective fuzzing must account for how much of the target application has been touched. If a file format is compressed, and the fuzzer only corrupts the compressed file itself, it is unlikely that the fuzzer will be impacting many of the important logic decisions the application makes based on the contents of the compressed format. Modern reverse engineering techniques, then, place an important emphasis on the completeness of the execution flow through an application.

Completeness metrics alone don't help. While they provide the map of yet-to-be-explored territory, the search space can be huge and the variety of corrupted inputs wide. Therefore, technologies must often scale to large numbers of nodes before they can produce useful results in any reasonable time frame.

Raytheon's Cutting Edge

Automation, completeness and scale are all important components in an effective reverse engineering process, but they come with their own drawbacks and implementation problems as well. Fortunately, Raytheon is ahead of the curve. The company began walking this path during the past five years and has made great strides in not only implementing solutions that take these approaches into account, but also resolving the practical implications.

Automating reverse engineering tools is in some ways straightforward. It's a simple programming exercise to expose a reasonable automation interface. What is much more difficult is automating the learning process — the interpretation of results to focus efforts on the most fruitful segments of code. Most approaches described in public literature for advanced automation are fragile, unworkable or merely theoretical. Raytheon SI's reverse engineering tool set — based on the Kernel Mode I^2 full-state tracking virtualization platform — offers an extensive API for integration into a variety of applications and a number of advanced features such as dataflow tracking, rewinding, unlimited differential snapshotting, and many others.

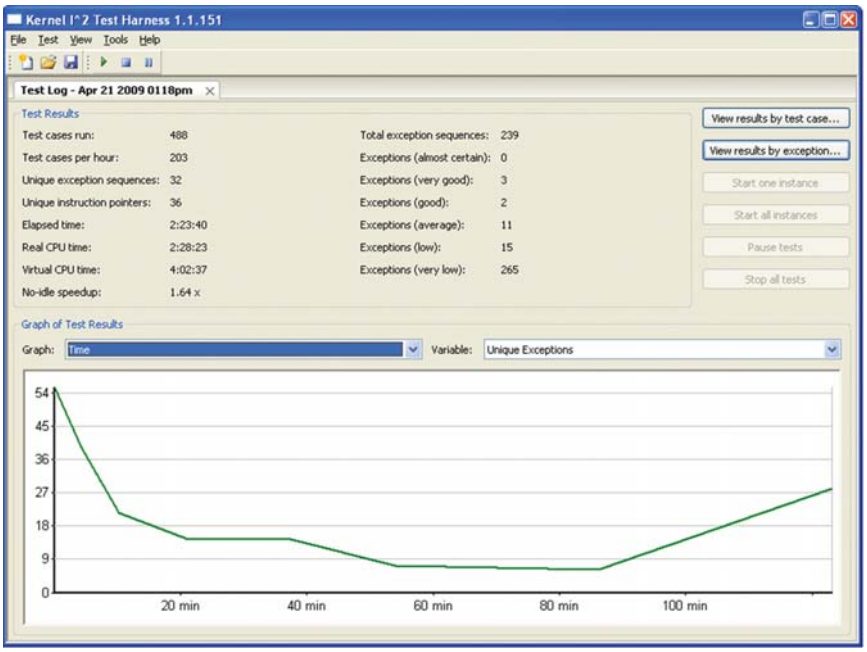


Figure 1. Automated Test Framework Showing Results Over Time

To address issues of completeness, a reverse engineering process must be able to instrument the application being executed. While application instrumentation is often accomplished with a debugger, that technology simply isn't powerful enough for detailed code-coverage analysis of modern applications. Existing public instrumentation tools capable of analyzing program execution down to the instruction level are much slower than Raytheon SI technology based on the internal Kernel Mode I^2 tool.

The most basic and efficient way to improve scale is to add more machines and add some basic command and control functionality for parallel processing problems like fuzzing a binary, but such a solution produces its own problems. One consequence is the volume of data produced. Simply increasing the amount of data produced by an automated process does not necessarily help make humans better at their tasks. A corresponding suite of advanced analysis tools must be built to handle the increased results, whether they're more crashes from fuzzing or more information about program code coverage. Figure 1 illustrates one important capability of our automated analysis. The graph — taken during a fuzzing test — plots the rate of unique exceptions discovered over time. A steady decline would be a sign that this test has exhausted the range of errant behaviors, but the upturn in this example indicates that it may be worth continuing. Note in the top center that we have automated the initial assessment of the risk associated with each exception.

While the state of the art has advanced in recent years, there are a huge number of potential spots for growth, and Raytheon SI is proud to be leading the way in identifying advancements in reverse engineering solutions to help identify and remediate vulnerabilities. ●

Jordan Wiens
jwiens@sigovs.com

ENGINEERING PROFILE

J.P. Leibundguth
Principal Scientist, NetOps and Information Solutions, NCS

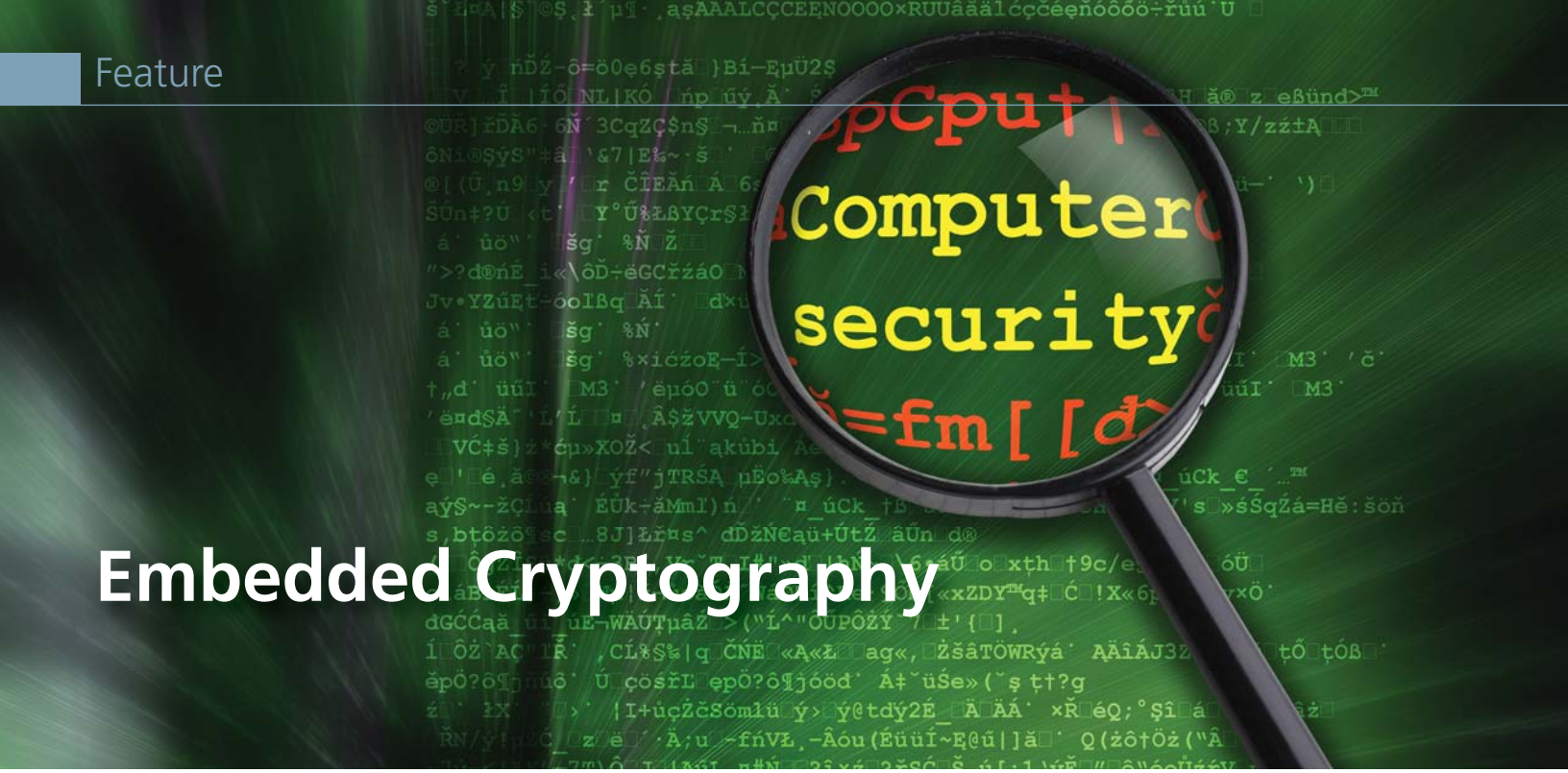
J.P. Leibundguth brings to Raytheon more than 12 years of research, software engineering, and consulting experience in the defense and commercial sector. As principal scientist at Raytheon NetOps and Information Solutions (NIS), his recent work is focused on network operations, information assurance, cyberwarfare, and related command and control capabilities. He works on NIS' healthcare-focused capabilities, programs and information systems.

Leibundguth supports information operations/information assurance innovation at Raytheon with special attention to advanced visualization techniques for cyberwarfare. He developed the CyberBML and NetManeuver concepts as part of Raytheon's Information Assurance Enterprise Technology initiative. As program engineer for the Defense Information Systems Agency (DISA) Multinational Information Systems Design, Transition, Operations contract, he leads the engineering and convergence of coalition warfighting networks spanning 82 nations, using Raytheon's Compartmented High Assurance Information Network technology.

"In the cyberwarfare domain, adaptive planning isn't just nice to have for future combat, it's a fundamental requirement, and its impact permeates nearly all of the capabilities we rely on for national security," Leibundguth said. "Raytheon takes it seriously, taking important steps to position itself with the best technologies, partnerships, acquisitions and capabilities for information assurance."

Before coming to Raytheon, Leibundguth served as a technical advisor for Joint Forces Command's Adaptive Planning and Execution Focus Integration Team. While at JFCOM, he also led functional concept, technology insertion, and experimentation activities in the field for the J9 force projection experimentation office. He has served as technical lead for software development programs, at the Pentagon, DISA, JFCOM and an intelligence agency.

His work on Java™ enterprise pattern innovation was published in "Dr. Dobb's Journal," and he received the prestigious Excellent Contractor Service Award, issued by the Director of Naval Intelligence, for the design, development and deployment of the Maritime Intercept Operations application in 2005.



Embedded Cryptography

Information assurance is defined by the processes and technologies required to manage the risks of storing and sharing information. Cryptography, a subset of information assurance, includes the technologies deployed to ensure the protection of sensitive information. Cryptographic methods are an esoteric blend of mathematics and computer science. Within the U.S., these methods and techniques are strictly controlled by the National Security Agency.

Raytheon produces a variety of communication systems that include embedded cryptographic technologies certified by the NSA for use in classified applications. Many of these systems use different cryptographic engines — each NSA-certified — but employ disparate technologies that have evolved independently as their program needs matured over the years. These products are referred to as Type 1 products. Type 1 is defined as a cryptographic system approved by the NSA for handling U.S. government-classified information.

The Type 1 certification process shown in Figure 1 is very rigorous and includes the creation of dozens of complex documents specific to a particular crypto embedment. It may span two to three years, and it requires a close working relationship with the NSA. Several Raytheon products have been certified using this process, with more in the pipeline. Every step in the process thoroughly analyzes minute details of a design to ensure minimal risk of inadvertently transposing classified information on an unclassified signal path. Typically, once a system has been certified, there is little desire to repeat this process.

Introducing Crypto Modernization

If changes are required in a crypto design or production process, this certification process must be repeated. Whether tailored or not, new certification requires serious time, engineering and funding. Because of this, Raytheon embraced software-defined cryptography and extreme commonality across its various product lines, with a goal to reuse hardware, software, firmware and certification documentation to minimize cost, schedule and risk for new certifications. This adaptability allows for rapid incorporation of new cryptographic algorithms, key management services or undefined capabilities yielding a future-proof design.

The NSA has defined new requirements for crypto modernization in NSA/CSS Policy 3-9 to include six basic tenets:

1. Assured security robustness
2. Cryptographic algorithm support
3. Interoperability
4. Releasability
5. Programmability
6. End crypto unit management and key management infrastructure compatibility

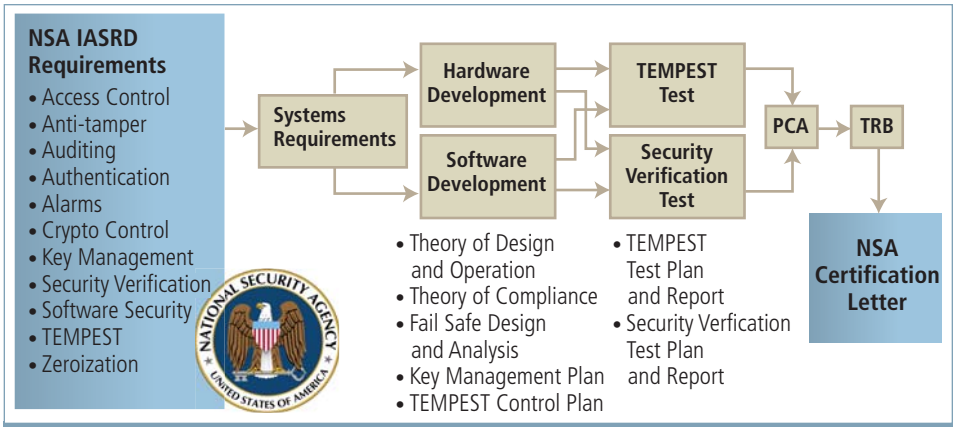


Figure 1. The NSA certification process often takes two or three years to complete.

This new agency mandate requires that Raytheon's existing suite of Type 1 products must be "crypto modern," driven largely by the retirement of old crypto algorithms in favor of new, highly robust algorithms. Raytheon has the opportunity to upgrade its legacy application-specific products to be capable of running new, sometimes yet-to-be-defined algorithms. This provides both an opportunity for growth and a technology challenge, as many of these products use different cryptographic engines and techniques to achieve NSA certification.

Developing a Reference Architecture

To prepare for this challenge, Raytheon developed a Cryptographic Reference Architecture to guide programs toward a common crypto solution by providing the desired hardware, software, firmware and certification documentation reuse.

Raytheon's unique position in the embedded crypto market is the diversity of solutions employed to achieve Type 1. Rather than relying on our own organic crypto engine solution, we tailor the selection of the engine to our unique requirements. In doing so, our embedment skills span technologies beyond a single device family and include devices from a variety of suppliers and competitors. We have exploited this knowledge to create the reference architecture and the common designs emerging from it.

Raytheon has successfully deployed the reference architecture on one high-profile system and used it to win the highly competitive F-22 Raptor KOV-50 Cryptographic Processor contract. The F-22 capture resulted in an Excellence in Business Development award, while the team that developed the reference architecture received a Raytheon Excellence in Engineering and Technology award.

Creating Benefits

Imagine the benefits of a common set of programmable, crypto modern solutions that can be reused across airborne, ground/vehicular, and man-portable Type 1 product lines: improved time to market, guaranteed interoperability, reduced unit costs, and Mission Assurance. All are achievable through this unusual level of commonality, saving millions of dollars and man years of effort for each Type 1 embedment.

Raytheon is emerging as a premier provider of embedded Type 1 cryptographic solutions. The diversity of our embedded cryptographic solutions; the multiple product domains we satisfy; the unique skill sets commensurate with Type 1 certification; our NSA-certified embedment specialists: All of these combine to provide growth opportunities in the new crypto-modernization market. ●

Larry Finger
larry_b_finger@raytheon.com

Cryptographic Product Types

Type 1 Cryptographic equipment, assembly or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information. Used to protect systems requiring the most stringent protection mechanisms.

Type 2 Cryptographic equipment, assembly or component certified by NSA for encrypting or decrypting sensitive national security information. Used to protect systems requiring protection mechanisms exceeding best commercial practices, including systems used for the protection of unclassified national security information.

Type 3 Unclassified cryptographic equipment, assembly or component used for encrypting or decrypting unclassified sensitive U.S. government or commercial information, and to protect systems requiring protection mechanisms consistent with standard commercial practices.

Type 4 Unevaluated commercial cryptographic equipment, assemblies or components that neither NSA nor NIST certify for any government use.

Source: Committee on National Security Systems, National Information Assurance Glossary, June 2006, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.

ENGINEERING PROFILE

Scott Chase
Technical Director, Raytheon SI Government Solutions

As technical director for Raytheon SI Government Solutions, Scott Chase actively promotes information operations and information assurance. Along with presenting SI's capabilities to internal Raytheon programs and customers, he helps to develop the next generation of offensive and defensive cybercapabilities for Raytheon, and to recruit and train future cyberprofessionals.

For Chase, interest in computers and security came at age 10, when he bought his first computer, a TI-99 clone with 16K of memory, from a discount store. He quickly learned BASIC and wrote programs to show his family and friends. His interest led him to enroll in the computer science program at Florida Institute of Technology. While at FIT, he became involved in student research, helping to start the Software Engineering Society and the Center for Information Assurance with Dr. James Whittaker. After graduation, he stayed on to work at the center full time.

In late 2001, security was becoming an increasingly important problem for companies and the government. However, the dot-com collapse meant few investors were interested in a software startup. Despite the risks, Chase joined Whittaker, former Lockheed Engineer Terry Gillette and others in forming Security Innovation in the fall of 2002, becoming director of security testing.

In 2005, SI Government Solutions was created to focus on a growing market — the information security needs of the U.S. defense industry. Around this time, Chase began collaborating with fellow researcher Herbert Thompson on "The Software Vulnerability Guide." The book, published in June 2005, was designed to teach developers how programming mistakes can lead to security vulnerabilities in software.

Chase was excited by the opportunity to sell SI to Raytheon in 2008. "As a small business, we were reaching the limits of what we could do on our own," he said. "With Raytheon's backing and access to government programs, we can achieve success in the information operations domain that wasn't possible otherwise." The team's efforts to defend U.S. cybersecurity were recently featured in "The New York Times" and other newspapers.

Quantum Cryptographic Networks

Quantum cryptography, more aptly named quantum key distribution (QKD), has emerged as a new paradigm for high-speed delivery of encryption key material between two remote parties. Typically, the security integrity of key exchange protocols is rooted in either a trusted third party, such as a trusted courier for symmetric encryption protocols, or the hypothesized computational complexity of one-way mathematical functions, such as the RSA encryption protocol.

QKD derives its security from the fundamental physical laws of quantum mechanics, affording the capability to remove from security proofs many of the assumptions about the capabilities of eavesdroppers in a public channel. In 2003, as part of the DARPA QuIST program, BBN Technologies deployed the world's first quantum network in metropolitan Boston and demonstrated how quantum cryptography can be used as an important tool in securing the world's most critical information-carrying networks.

The QKD Protocol

QKD uses a single quantum particle as the physical medium on which to encode a single bit of key material. A quantum particle encoded with information is referred to as a quantum bit, or qubit. The quantum mechanical nature of these particles exhibit two uniquely quantum physical characteristics which make the encoded information robust against interception by eavesdroppers:

- Quantum particles are indivisible units of energy, so they cannot be divided by an eavesdropper for passive monitoring.
- Quantum particles are subject to the Heisenberg uncertainty principle, so measurement of a quantum particle by an eavesdropper irreversibly alters the state of the particle, yielding an effect that is noticeable to the two communicating parties.

While there is a broad spectrum of implementation techniques for performing practical QKD, there are overarching commonalities to all the protocols and techniques. Figure 1 shows a system-level schematic. A designated sender and receiver have distinct roles in the protocol.

To begin the negotiation of a secret key, the sender prepares a single photon for transmission to the receiver by generating a bright laser pulse and attenuating the pulse to an intensity much less than one photon per pulse, ensuring that very rarely a data pulse exits the transmitter that has two photons that would provide an eavesdropper with excess information. Next, the transmitter randomly encodes two bits of information on the photon from a set labeled Φ_S, and the encoded photon is directed into the transmission channel. The information can be encoded in any measurable quantity of the photon such as electric field polarization or optical phase.

The transmission channel can consist of any transparent medium, whether it is free-space or fiber-optics. For long-distance, high-data-rate communications,

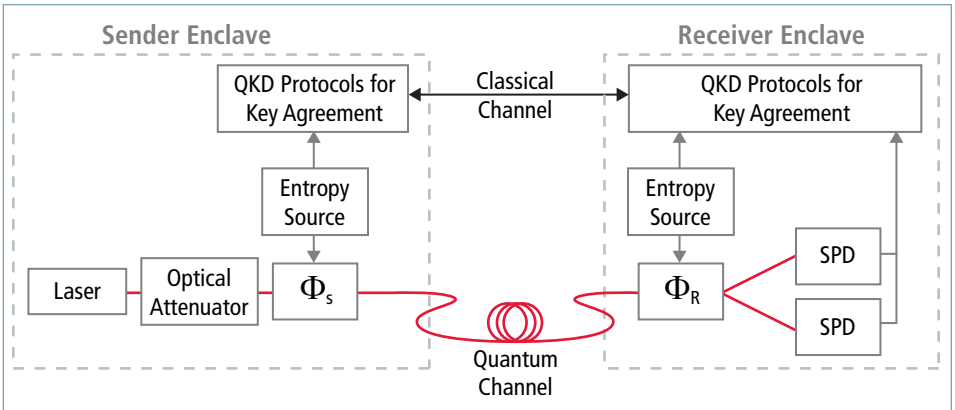


Figure 1. A system schematic for a point-to-point QKD link

telecommunications-band optical fiber is often the channel of choice. As photons enter the receiver from the channel, the receiver randomly chooses a measurement basis, from one of two choices Φ_R, in which to measure the photon, and then performs photon counting with two single photon detectors (SPDs).

The sender and receiver repeatedly execute this protocol and monitor the error rate of the resulting bit streams. Since any interrogation of the photon in the channel by an eavesdropper alters the state of the quantum bit, the presence of an eavesdropper can be detected as an increase in the error rate of the communications, as tested through error detection routines for the protocol utilizing an unsecured classical communications channel.

The DARPA Quantum Network

In 2003, in collaboration with Boston University and Harvard University, Raytheon BBN Technologies deployed the world's first quantum key distribution network in the metropolitan Boston area[1]. A multidisciplinary team of physicists, software and hardware engineers, and network architects designed and built the quantum network. QKD nodes at each university were connected to BBN via dedicated optical fiber channels and networked through an optical switch located in the laboratories at BBN. In addition, several variant QKD systems were integrated into the network, including free-space and quantum-entanglement-based links.

The system was engineered to operate without manual intervention, continuously generating key material shared between pairs of locations. A critical component to the project focused on integrating QKD with the security protocols for network communications that are currently used. BBN developed a suite of protocols for key negotiation, as well as the integration of key material into protocols such as IPSec, commonly used for secure communications on the Internet.

The Future of Quantum Networks

Since the deployment of BBN's quantum network, several other demonstrations have emerged around the world. Perhaps the most recent is the deployment of the European SECOQC network[2] in Vienna, integrating several QKD technologies into a ring topology network. The European network has addressed the important issue of network scalability by forming a trust model between intermediate nodes in the network through which key material flows. Ultimately, for quantum networks to scale without such a constrained trust model, it requires the integration of quantum entanglement sources and quantum memories to construct quantum repeater stations at intermediate nodes between users, and Raytheon BBN Technologies is pursuing these technologies.

QKD has been demonstrated as a practical and useful tool in securing critical communication networks. Important challenges lie ahead, including increasing key exchange throughput, and extending reach and compatibility with currently installed fiber networks that are not optically transparent from user to user. Continued research on quantum-based sources, detectors and processing subsystems is aimed at addressing these challenges. ●

Jonathan L. Habif
jhabif@bbn.com

[1]C. Elliott, D. Pearson and G. Troxel, "Current status of the DARPA quantum network," Computer Communication Review, v. 33, n. 4, p. 227–238.
[2]www.secoqc.net

ENGINEERING PROFILE

Jonathan Habif
Senior Scientist, Raytheon BBN Technologies

As a senior scientist at Raytheon BBN Technologies in Cambridge, Mass., Jonathan Habif focuses on the applications and development of quantum information system sciences. He has been a technical lead for the DARPA Quantum Network program and a principal investigator on the DARPA Quantum Sensors Program, now entering its second phase. In 2007, he received the Anita Jones Award for classified work introducing a new technology to BBN.

"Our group works to develop technologies that many think are not possible," Habif said. But, he added, current research in the field shows that much is possible. "The field of quantum information is in its adolescence, but already applications of quantum mechanics, such as quantum cryptography, have yielded strong evidence that important discoveries and radical new technologies are within our grasp."

His graduate work in applied physics helped spark his interest in challenging the possible, Habif said. "As a graduate student I was keenly interested in controlling and measuring the quantum mechanical state of devices in which quantum effects had never been observed."

With the rapid progress made in these fields in the past decade, he added, physicists and information theorists can design and build systems that capitalize on the quantum coherent properties of devices. "It is a historic convergence of physics and engineering, and BBN has boldly set out to understand the fundamental issues that need to be addressed and advantages that can be attained."

In 2000, Habif was awarded a NASA GSRP fellowship for his graduate work investigating quantum coherence in superconducting circuits. He was a postdoctoral research member of the MIT physics department from 2003 to 2005, focusing on the development of the integration of classical control circuitry with superconducting quantum coherent devices.

Information Assurance for Communication Systems

Innovative technologies to protect warfighter data in transit

Comprehensive Mission Assurance requires secure battlefield communication. Warfighters must be confident that their data meets the three main tenets of information assurance: confidentiality, integrity and availability.

Although classic IA technologies such as firewalls and network intrusion detection and prevention systems are used in a defense-in-depth manner, they typically do not secure the internal data that is being communicated. Firewalls monitor and limit network connections. Network intrusion detection systems scan network traffic to detect malicious actions and intent. Because these technologies are applied at network boundaries, additional technologies must be used to ensure the confidentiality and integrity of the data being communicated.

To meet this challenge, Raytheon recently funded IA research into Internet Protocol version 6 (IPv6), High Assurance Internet Protocol Encryptors (HAIPE), and a Common Cryptography Module Architecture. These technologies provide encryption and other safeguards to ensure that data gets to the correct individuals without being modified or intercepted. These logical controls, described below, help to support the goal of Mission Assurance in military communication.

IPv6

IPv6 is a network layer for packet-switched internetworks. It is designated as the successor to IPv4, the current version of the Internet Protocol, for general use on the Internet.

The emergence of IPv6, providing the world with an exponentially larger number of available IP addresses, is essential to the continued growth of the Internet and development of new applications leveraging mobile Internet connectivity.

In addition, IPv6 contains additional functional and security capabilities beyond that offered by IPv4. However, added features introduce other issues. IPv6 supports addresses that are 128 bits in length, which provides for about 3.4x1038 possible IP addresses. This capacity allows a unique IP address to be assigned to every device on the planet — including your toaster — thereby eliminating the need for network address translation. NAT has provided residual security benefits by shielding a user's private address space from direct contact with the outside network. NAT routers are commonly used by households today because they allow multiple computers to share a single IP address. A NAT router limits direct access to the household's computers. With IPv6, direct access to an IP address is allowed and this creates security implications, such as the potential for targeted denial of service attacks.

IPv6 offers enhanced capabilities such as mobility through the use of Mobile IP v6, which allows an IPv6 node the ability to retain the same IPv6 address regardless of

its geographic location or the equipment to which it is connected. Moreover, IPv6 includes improved quality-of-service features that reduce packet header processing overhead and employ traffic class and flow label header fields that expedite packet priority handling. More important to this discussion, IPv6 offers inherent end-to-end security services that include entity and data origin authentication, connectionless integrity, replay protection, data confidentiality, and limited traffic flow confidentiality.

IPv6 provides end-to-end confidentiality by enabling end nodes to create a mutual security association through the network. Figure 1 represents a simple end-to-end path over a network, with the end nodes' addresses expressed in the IPv6 format of eight groups of four hexidecimal digits. The security association is established between the nodes using a shared secret that is either preconfigured or generated dynamically using cryptographic key agreement algorithms. IPsec implements standard cryptographic algorithms and protocols to authenticate the nodes, ensure authenticity and integrity of messages, and prevent traffic flow analysis.

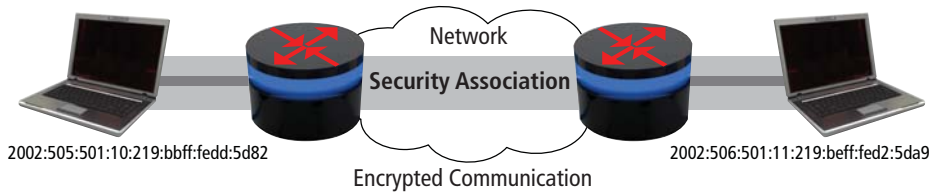


Figure 1. Secure Network Communication

Encryption used to secure classified information is referred to as Type 1 encryption. Type 1 encryption products are subject to advanced levels of validation, verification and certification throughout their life cycle. In recent years, Type 1 standards have been developed for IPsec-style IP datagram security services. A HAIPE device is a National Security Agency (NSA) Type 1 cryptographic product that provides IA services for IP data-in-transit.

HAIPE

The foundation of HAIPE is its use of subsets and custom variants of Internet Engineering Task Force IPsec standards and protocols for the purposes of enhancing cryptographic algorithms and capabilities. HAIPE foreign interoperability (HAIPE FI) capability provides the ability to safeguard IP communications in different operational environments though its use of NSA-approved classified (Suite A) and unclassified (Suite B) algorithms.

HAIPE FI capability is available in HAIPE IS versions 1.3.5-FI and 3.x. HAIPE FI includes an exclusion key (EK) capability that enables the creation of dynamic communities of interest (COIs) with two levels of cryptographic protection: one through an asymmetric key exchange, and one through the addition of the symmetric EK. COIs are created by configuring HAIPE peers to require the use of an EK for certain communications (e.g., policy-based), and selectively loading that EK on the appropriate HAIPE peers. See Figure 2 for examples of using exclusion keys in COIs.

Through Raytheon's research, the company has collaborated with the NSA to define the IA policy and guidance for HAIPE use within the U.S. Department of Defense.

Common Crypto Module Architecture

Further extending Raytheon's research into HAIPE technology, a Common Crypto Module Architecture was developed to modularize system components of a radio frequency circuit board. The Common Crypto Module Architecture provides Type 1 and HAIPE functionality to RF communications. Radio builders can leverage this architecture to furnish government-certified encryption to their military communications. This modular architecture allows the capabilities that best fit the system concept of operations.

These are some of the main technologies for ensuring that warfighter communication and data are secure. All of these technologies enable seamless IA that empowers rather than hinders the user. •

Randall Brooks
randall_s_brooks@raytheon.com
Contributor: Chris Rampino

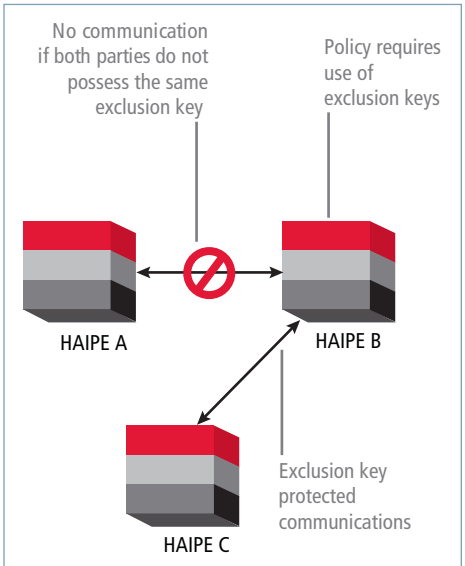


Figure 2. Exclusion – Key Protected COIs

Attack and Defend in Cyberspace – and Within Raytheon

"Attack and defend in cyberspace" took on a new meaning within Raytheon last year through the Information Operations Enterprise Initiatives. Raytheon engineers from across the company embarked on a mission to fulfill two major requirements:

1. Demonstrate the ability to attack and defend in cyberspace
2. Demonstrate the ability to connect cybereffects to physical effects

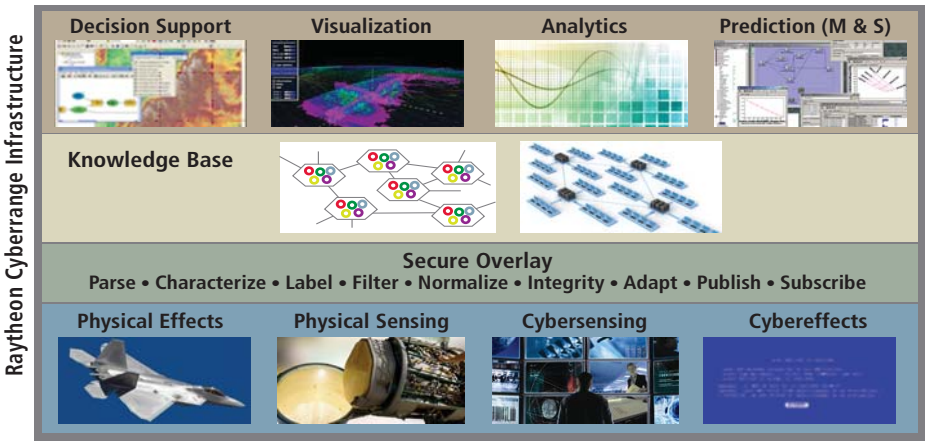
Addressing Customer Concerns

In discussing cyberspace with current and potential customers, it is apparent they have a strong desire for one of their trusted partners to step to the front with a demonstrable capability that addresses their concerns with regard to protecting the cyberdomain. For some entities, the defense of their networks is the primary concern. For other entities with Title 10 or Title 50[1] authority, the ability to provide active defense widens the aperture.

In a recent meeting, a Raytheon customer stressed the need to be able to actively visualize enterprise resources through complete cyber situational awareness faculties, track intrusion attempts, perform forensic analysis, and — when the threat reaches a predefined threshold — execute a precision response using a tool box of cybereffects. The enterprise initiatives developed a demonstration scenario that will be used to highlight our ability to meet our customer's need.

Raytheon excels at defending and securing cyberspace for our customers. But what about attack? This is a more difficult problem to address. First, in order to attack, one has to have a target and the authority to launch an attack on the target. However, Raytheon lacks the authority to launch an attack, as only certain entities within the government possess the Title Authority to prescribe cyberoffensive maneuvers. Second, many of the cybereffects we develop for our customers are locked in classified vaults and cannot be brought into an open environment.

To address customer concerns, Raytheon has developed a representative architecture.



Architecture

The architecture provides a layered approach driven by cybersensing and effects as well as physical sensing and effects. These lower level entities depend on the "plumbing" provided by the secure overlay layer to parse, (potentially) label, filter and normalize the data provided to the knowledge base. The knowledge base provides the engine for the architecture and interacts with decision support (sometimes referred to as command and control). The knowledge base provides data for the analytics engine and the visualization engine. Modeling and simulation capabilities are provided through the prediction component. The demonstration will eventually reside in the Raytheon Cyber Tactics Center.

Cybersensing

Three projects are being delivered under the cybersensing umbrella. The Botnet Discovery project will develop a system that actively seeks out command and control systems of botnets. The Active Enterprise Security Platform project will develop a common execution and data integration environment for deploying command-line tools to support both computer network defense and computer network operations. In conjunction with Active ESP, the Computer Network Attack and Response project will develop a prototype system that can detect an attack and actively formulate and deploy a response.

Cybereffects

Because of the secure nature of many of the cybereffects in Raytheon, a primary focus of the cybereffects projects is the development of unclassified non-kinetic computer effects that can be used as demonstrable evidence of Raytheon's capabilities in this area. Projects focus on different types of effects, including polymorphic agents, rootkit exploitation techniques, hypervisor rootkits, the use of steganography to produce an effect, and the ability to persist the effect within a computer or network. Effects are being developed in many areas and include the capability to destroy, degrade, deny, deceive and disable assets and/or operations. On the flip side, research is being conducted to counter the technical threats to the effects being generated. This dynamic, coupled with the cybersensing projects, will provide an active offense versus defense scrimmage capability.

In Melissa Hathaway's Cyberspace Policy Review delivered to President Obama in May 2009, she noted that "The growing sophistication and breadth of criminal activity, along with the harm already caused by cyber incidents, highlight the potential for malicious activity in cyberspace to affect U.S. competitiveness, degrade privacy and civil liberties protections, undermine national security, or cause a general erosion of trust, or even cripple society."[2]

Cyberattack is real and the consequences of not being prepared are severe. Through the diligent work of engineers across the company, the Information Operations Enterprise Initiatives scenario will transform from an intriguing story to a live demonstration of some of the most advanced cybereffects in the world today. ●

Rick Butler
rick_butler@raytheon.com

[1]Title 10 Authority gives a government entity the authority to launch a cyberattack on an adversary. Title 50 Authority allows a government entity to perform computer network exploitation.
[2]"Cyberspace Policy Review," Page 2, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

Beyond Probe and Patch:
A Case for Intrusion-Tolerant and Self-Healing Approaches to Cybersecurity

Mission- and safety-critical systems require a very high degree of reliability and availability, typically measured in many nines. Examples of such systems include command and control, fire control, and weapon control systems in the military domain, as well as numerous civilian systems such as air traffic control, power grid controls (SCADA) and power plant controls. Consequences of data corruption or a shutdown of these systems have the potential to cause significant loss of life, commerce or military objectives.

When it comes to accidental hardware component failures and software malfunctions, these systems are designed to be robust and fault tolerant, and able to recover with minimal operator intervention and no interruption in service, while maintaining absolute data integrity. But this is not the case when it comes to malicious attacks, where the approach is still focused on preventing intrusions and hardening the systems to make them as impenetrable as possible.

Mission-critical systems are facing increasingly sophisticated cyberattacks. Our nation needs to develop novel technologies that enable systems to recover and reconstitute in real time, and continue to operate correctly after an attack. For the past five years, Raytheon has been conducting research into intrusion-tolerant and self-healing systems as part of its internal research and development, as well as in partnership with its U.S. government customers.

The Current State

One problem is that the number of software vulnerabilities is innumerable and growing constantly. The Common Vulnerabilities and Exposures (CVE) database currently contains more than 36,000 unique vulnerabilities. Even a secure operating system such as SELinux has 15 identified software flaws (as of July 2009). The threat posed by these vulnerabilities is asymmetric; defenders must close all holes, while the attackers need to find only one. However, it is impractical to probe and patch every single defect. Unlike random hardware faults, the probability of occurrence of this event cannot be modeled stochastically, because a single undefended but exploitable vulnerability creates a modeling singularity. So it is hard to quantify probability of mission success or failure for a system that relies solely on preventive methods.

In addition to software flaws, systems also suffer from configuration errors. These are even harder to control as systems are continually upgraded and components added, deleted or modified. What about the argument that a system is less vulnerable if it does not use commercial off-the-shelf software but has high-assurance, validated software? In fact, the most highly tested mission-critical software, such as the Space Shuttle flight control software, was still found to have about one error per 10,000 source lines of code. Most military command and control systems do not go through such rigorous testing. The conclusion is that technology does not exist today to design, code, test and deliver defect-free software for a system of realistic complexity, and it is not likely to be available in the near future.

Another argument usually put forward in favor of preventive measures is that military systems are inaccessible to unauthorized users, and access control mechanisms are sufficient to keep intruders out. This would be the case if physical access or remote login access were the only means of getting inside these systems. Any networked information system has many entry points, and boundary controllers are not completely effective in separating malicious activity from normal traffic. For example, it is difficult to identify hidden scripts in legitimate documents. Furthermore, where humans are concerned, one should not underestimate the power of social engineering in bypassing access control mechanisms. As a result, it is prudent to assume that penetrations of multiple layers of defensive layers are not only possible but quite likely, especially if the threat is a goal-oriented, well-resourced and determined adversary.

In fact, that is why intrusion detection sensors are now routinely deployed not only at network gateway points, but also in internal routers and on hosts, servers, and more and more end devices. What is the efficacy of current intrusion detection sensors? The most common principle is to look for a

Continued on page 28

Continued from page 27

signature of malicious code by matching bits to known fragments. This has an obvious limitation of not being able to detect novel attacks. Even minor variations of known viruses can escape detection. Keeping such sensors up to date in light of a daily onslaught of new variants is a burdensome task. New attacks must be caught, their code analyzed, a signature created, and pushed out to all target machines as soon as possible to close the window of attack vulnerability. This task is even harder than probing and patching vulnerabilities because of the infinite number of mutations of a virus. A less common principle of detecting intrusions is to detect anomalous behavior. This assumes that it is possible to define normal behavior. Except for some very simple, deterministic state machines, it is extremely difficult to specify the bounds of normal behavior that will never be breached. That is why anomaly detection sensors have unacceptably high false-alarm rates.

Therefore, preventive layers will be penetrated by a determined adversary, and detection layers may, or may not, detect such an event. This is a very realistic scenario for today's mission-critical systems.

A Paradigm Change

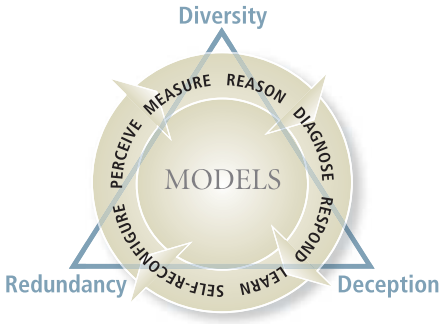
Almost all research and development on cybersecurity is still aimed at preventing and detecting intrusions. This paradigm must change and U.S. government officials at the highest levels are coming to the same conclusions, as noted in a "New York Times" article about a review of the nation's cybersecurity conducted for the Obama administration by Cybersecurity Advisor Melissa Hathaway:

"As Mr. Obama's team quickly discovered, the Pentagon and the intelligence agencies both concluded in Mr. Bush's last years in office that it would not be enough to simply build higher firewalls and better virus detectors or to restrict access to the federal government's own computers."

"The fortress model simply will not work for cyber," said one senior military officer who has been deeply engaged in the debate for several years. "Someone will always get in."[1]

The question now is: What do we do when, not if, a system has been penetrated due to a cyberattack?

One course of action is to take an offensive approach and strike back to neutralize the threat if it is possible to trace the attack back to the perpetrator whether a non-state actor or a nation-state.[2] Developing an offensive capability may also serve as a deterrent — at least for nation-states, if not for terrorist organizations. However, the focus of this article is on the defense of our networked systems.



In this representation of an approach to self-healing information assurance, the triangle's apexes show the key elements of such an approach, while the circle shows the recurring steps that must be taken – from measurement to reasoning to learning – in order to infuse systems with cognitive capabilities to survive cyberthreats.

The defense-in-depth strategy requires augmenting the prevention and detection layers with the next logical mechanisms that allow systems to recover from attacks, repair the damage and reconstitute their full functional capabilities in real time or near-real time for mission-critical systems, and with minimal human involvement. Systems that have such properties have been called intrusion-tolerant systems and self-healing systems.

An intrusion-tolerant system continues to perform all critical functions and provide the user services it was designed for, even in the face of a cyberattack. A self-healing system goes further and purges itself of the malware just as a biological entity neutralizes an infection. This ensures that all compromised components are infection-free. It repairs all damaged databases just as a biological system heals wounds and grows new tissue. This process reconstitutes full functional capabilities as existed prior to attack.

Starting in 2003, several DARPA programs explored a number of novel ideas, including redundancy, artificial diversity, randomness and deception, among others. Along with Cornell University, Raytheon participated in a DARPA program to develop technology for self-regenerative systems. In 2008, Raytheon received a DARPA contract to evaluate the effectiveness of new technology for countering cyberthreats from inside users. Details of DARPA's research projects can be found at http://66.255.97.26. Some of the fundamental concepts that came out of the DARPA programs are described in the book "Foundation of Intrusion Tolerant Systems," published in 2003 by IEEE Computer Society Press.

Until industry and government are able to design and build defect-free and vulnerability-free components, intrusions will occur, and some of them may not even be detected. For mission- and safety-critical systems, it is paramount to architect them from the ground up so that in the event of a cyberattack, they continue to function correctly, keep data integrity and continuity of service for critical functions in real time, and reconstitute full functionality over time. ●

Jay Lala
jay_lala@raytheon.com

[1] Sanger, D.E., et al., U.S. Plans Attack and Defense in Cyberspace Warfare, "The New York Times," April 28, 2009.
[2] Owens, A. W., et al, editors, "Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities," The Computer Science and Telecommunications Board, National Research Council, Washington, D.C., May 2009, www.cstb.org.

For Your Eyes Only:
Ensuring Authorized Access to Computer Information

Raytheon is currently working on two innovative technologies — Location Aware Access Control and Persistent Log on — that will ensure user authentication in a secure computing environment. The technologies will be feasible for commercial use in hospitals, banks, retail and manufacturing, as well as military and civil markets — including command and control, weapons systems and border security.

The Scenario

A multinational task force is formed in response to emerging hostilities in the Horn of Africa. U.S. Marines are tasked with forming a tactical operations center (TOC) to provide coalition command and control systems for British, Japanese, and African Union commands. Yet classified U.S. information must still be processed in the same facility to facilitate time-critical information sharing.

Working within the same room, how can U.S. forces effectively prevent accidental leakage of sensitive data to allies? Tape off areas of the TOC and have non-U.S. persons stay on their side of the line? Turn computers and desks so that they cannot be seen by allied staff? Escort allies from the room when certain information is processed?

All are common and quite rational solutions for implementing physical control policies in this situation. However, if someone wanders out of his controlled area there is a very high risk of information being viewed or accessed by uncleared personnel during the transgression.

What if information systems were smart enough to prevent this form of leakage from occurring? As uncleared personnel approach an active terminal, several actions could occur. Screens could go black or display a screen saver. Keyboard input could be locked. Log-on capabilities could be locked out. Once the uncleared visitor leaves the physical or visual proximity of secured terminals, access could be returned to legitimate users.

The technologies to make this happen exist today within Raytheon. Location-aware access control can be achieved by correlating a user's physical location to that of the computers they log on to. Personnel can be identified through stand-off biometrics, and their movements can be tracked with a high degree of fidelity. Characterization of personnel interaction with physical assets can be achieved.

Through Raytheon's 2009 Innovation Challenge, two projects were identified that show the potential of enabling the technologies needed to build a system that addresses the problem.

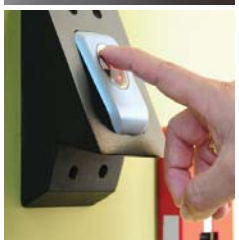
Location Aware Access Control

The first project, Location Aware Access Control, originates from a system that was successfully deployed within Raytheon to consolidate all badges, identifications, passwords, and personal identification numbers to a single set of credentials. Through this system, customers can enter access controlled doors, log on to computers and access Single Sign-On (SSO) services, using a single smartcard and fingerprint for identification and authentication.

Persistent Log On

Imagine a facility where, instead of each user logging in to their host computer, everyone logs in to an enterprise system that "owns" all of the access points (displays, keyboards, doors, etc.) and dynamically tailors access in real time. This type of ubiquitous computing is called "context-aware pervasive computing."

To establish a strong initial level of authentication, personnel will log in using a combination of smart cards, passwords and biometrics as usual. As people move through the facility the system captures video, voice and other biometric data that is analyzed and fused into real-time tracks. Privacy is assured by carefully separating identification from localization within the system. This fusion process also produces a confidence factor that is considered along with other-user contexts to dynamically grant access to the system.



Over time, confidence in a user's identity will degrade as he commingles with other employees, works in open offices or cubicles, or moves through areas that lack video surveillance, such as restrooms. Periodic challenges are issued when confidence levels decrease below a defined threshold, and users must present their smartcard and biometrics at physical access control points or computer terminals.

Context-aware pervasive computing makes the user's experience indistinguishable from magic. The user's session hops from computer to computer as the user moves through the facility: automatically authorizing entry to controlled areas, automatically presenting appropriate access windows on local machines, and automatically removing sensitive data from the screen when unauthorized users approach. The unified approach also facilitates activation of emergency systems states during distress conditions, and from a cyberperspective, provides an invaluable source of forensic data on insider threats. ●

Shane Powell
shane_powell@raytheon.com
Tim Smith
tdsmith@raytheon.com

Raytheon and West Point's Information Technology and Operations Center: Partnering to Defend the Cyberdomain

Raytheon's objective to provide its customers with comprehensive solutions in the area of information assurance and information operations has resulted in the initiation of valuable partnerships with several academic institutions that are pursuing research in these areas. A partnership with United States Military Academy at West Point's Information Technology and Operations Center (ITOC) was a natural choice for Raytheon, allowing the company to work in information operations with a top-notch research institution that also happens to be part of one of Raytheon's primary customer organizations: the U.S. Army.

The U.S. Military Academy at West Point has a storied history as the premier institution of military education in the U.S. Since it was founded by President Thomas Jefferson in 1802, the academy has been dedicated to providing the nation with "Leaders of Character" who can serve the nation in military operations throughout the globe.

The cadets who graduate from West Point in these early years of the 21st century face ever-more complex challenges as they enter the U.S. Army as second lieutenants. Among those challenges is the increasing need to protect our nation, and its military defenders, against cyberattack.

Responding to that challenge, West Point created ITOC in order to equip the Army to better deal with the looming challenges of information operations. The mission of the ITOC is "to educate and inspire cadets and faculty in the acquisition, use, management, and protection of information through innovative teaching, curriculum development, research, and outreach to Army, DoD, and federal agencies." As part of West Point's Electrical Engineering and Computer Science (EECS) department, the ITOC draws from a stellar faculty — many of whom bring experience as active-duty military officers, along with advanced degrees to their research endeavors.

In the fall of 2008, engineers from Raytheon's Corporate Technology and Research organization participated in discussions with ITOC faculty to identify research projects of common interest. In the early months of 2009, Raytheon's University Research Program funded two research programs at the ITOC.

West Point cadets engaged in a cyberattack exercise

The first research project is being conducted under the auspices of Raytheon's Intelligence and Information Systems (IIS) business. Titled "Secure Soldier Field Computer," this project will investigate the various software and hardware configurations that will be utilized in future field operation computers. Insight into these configurations will support identification and development of appropriate cybersecurity measures that can be used to protect the data and functionality provided to the soldier via these computers.

The second research project is sponsored by another Raytheon business, Network Centric Systems. Titled "Netted Secure Soldier Field Radio," this project will investigate new methods of providing soldiers with a low-weight secure radio that supports more rapid setup and is less cumbersome to use than currently fielded secure radios. Because these radios will need to function as part of a comprehensive netted communications system, the impact of a new approach to radio security to the overall communications infrastructure will also require investigation. The field-duty experience brought to this task by West Point faculty members will be invaluable in determining the viability of any type of secure radio in a "real world" setting.

Raytheon is also partnering with its U.S. Army customer by offering summer internship opportunities to West Point cadets. As part of West Point's Academic Individual Advanced Development program, several cadets learned and contributed at a number of Raytheon businesses during the summer of 2009. Two cadets with an interest in information operations spent a few weeks at IIS' SIGov affiliate in Melbourne, Fla. Four other cadets were in Tucson, Ariz., to participate in a summer internship sponsored by Raytheon Missile Systems. In an effort to further interservice communication, the RMS program partnered USMA cadets with cadets from the United States Air Force Academy at Colorado Springs, Colo.

The Raytheon engineers who work with the professors and staff at the ITOC are excited about this opportunity to engage in research that will benefit our company, the faculty and cadets at the United States Military Academy and, most importantly, the soldiers who serve our nation. ●

Jeanne Minahan Robinson
jrobinson@raytheon.com

Raytheon Partnerships Enhance Cyberdomain Research

Can game theory be applied to help us make smarter decisions in protecting critical infrastructure? Could it also help plan automated responses to deter attacks? Can intelligent software agents watch ad-hoc network nodes to catch untrustworthy behavior? Those are just a few areas in which Raytheon is sponsoring research at universities and small businesses.

Many past and current advances in the cyberdomain come from research started at universities or small businesses. Partnering with organizations involved in government science and technology research is a natural fit — they and their customers want strong transition partners to integrate promising technologies. Raytheon benefits by being among the first to pilot innovative cybertechnologies well before they enter the commercial mainstream. Raytheon recently sponsored a mini-symposium day, where many of the universities we sponsor in cyberdomain research shared their accomplishments with us and their peers.

George Mason University

Raytheon and George Mason University are working together on several projects. Elsewhere in this issue, you can read a description of CAULDRON, a software suite developed by GMU to help designers make smarter decisions about where to begin to secure a complex system. Raytheon is also evaluating an array of innovations from GMU, including their Self-Cleansing Intrusion Tolerance (SCIT) technology and Uninterruptible Server. Through different approaches, each of these technologies protects against successful intrusion by novel malicious code.

Raytheon has also worked to extend GMU's "Battle Management Language," exploring the use of natural language commands that can be interpreted by computer. While the time-tested system of military orders, tasks, requests and reports continues to provide positive control over forces, the pace of battle possible in the cyberdomain necessitates advances in automated tasking of both cyber and conventional forces. A battle management language (BML) formalizes command and control (C2) messages using unambiguous terms, rules and semantics. BML captures the prescribed rules and well-defined verbs and terms that are meaningful to each domain. For CyberBML, Raytheon is extending BML to include verbs, terms and structures that extend C2 into the cyberdomain. This approach is based on a generalized C2 model called Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM), developed by the NATO Multilateral Interoperability Programme.

Massachusetts Institute of Technology

Beyond the C2 cybermodel, there is the more practical challenge of moving information between IT and C2 databases. Raytheon accomplishes this by partnering with a team from the Massachusetts Institute of Technology and using its "M Language," which offers a technology-neutral dictionary, store and binding mechanism between databases. M Language also serves another purpose. Natural language orders, requests and reports are a key ingredient in any C2 system. With M Language, MIT has pioneered advanced natural language processing techniques that could eventually automate knowledge extraction from ongoing message traffic. This could be presented in CyberBML format for enhanced situational awareness and speed of command. The final, keystone component for a CyberBML capability is the CyberBML parser, written to adhere to the defined language and terms stored in the M Language dictionary. An initial version of the CyberBML grammar, terms and parser was developed at Raytheon in 2008.

University of Texas at Austin

Raytheon has partnered with The University of Texas at Austin's Center for Information Assurance and Security (CIAS) on research for new and innovative cybersecurity solutions. The 21 faculty members in CIAS, a research unit in the university's Department of Computer Science, bring significant technical knowledge specific to cybersecurity. During the next 10 years, Raytheon will provide funding for CIAS faculty working on computer security and information assurance projects. Initial efforts are focused on formal verification methods, and researchers there are addressing increasingly critical issues such as privacy, password cracking, network security, intrusion detection, verification and wireless networking.

"Protecting our nation's computing systems that control critical cyber infrastructure is crucial," said Dr. Fred Chang, lead investigator and director of the CIAS. "The partnership with Raytheon will allow us to expand our capabilities to address the rapidly changing problems in cybersecurity with a great deal of agility and flexibility."

University of Arizona

Understanding and measuring trust is an integral component of mastering information assurance. In order to model and create a metric for trust as it applies to information assurance, Raytheon is collaborating with Dr. Sudha Ram at the University of Arizona. Raytheon began working with Ram in 2005 when she won an National Science Foundation grant to model provenance in the context of complex material properties. She is a McClelland Professor of Management Information Systems in the Eller College of Management, and she is researching interoperability among heterogeneous database systems, semantic modeling and automated software tools for database design, among other topics.

Raytheon used this collaboration to create a knowledge management tool called the Material Property Management System to compile material property information and track complex provenance. Raytheon and an organization called Science Foundation Arizona funded continuing research as Ram began investigating how to measure data quality with the help of provenance.

Continued on page 32

Continued from page 31

Raytheon identified the applicability of this research to information assurance and trust metrics, which led to collaboration on data provenance and the use of provenance metadata to derive a trust value associated with the data product from a sensor. Raytheon is also exploring provenance metadata associated with entities (human users, services, software agents and devices) as they produce, transform or consume data.

Carnegie Mellon University

Raytheon is a partner of Carnegie Mellon University's CyLab Sustainable Computing Consortium. CyLab was founded in 2003 and is one of the largest university-based cybersecurity research and education centers in the U.S. It is is a National Science Foundation CyberTrust Center, a key partner in NSF-funded Center for Team Research in Ubiquitous Secure Technology, and a National Security Agency Center of Academic Excellence in Information Assurance Education and a Center for Academic Excellence in Research.

Raytheon and Carnegie Mellon collaborate on government, commercial and international opportunities and on advancing the state of cybertechnology. In current research, Raytheon is working with CyLab to anticipate the security challenges posed by the rapid adoption of virtual reality environments and to explore innovative technology solutions to identity management, rights management, and detection of untrustworthy behavior. Raytheon participated in the Sixth Annual CyLab Corporate Partners Conference in Pittsburgh.

University of Southern California

University of Southern California's Information Sciences Institute was formed with DARPA support in 1974 as an outgrowth from Rand Corporation. ISI helped to build the original Internet, developed the domain naming service, and the protocols Kerberos and RSVP. ISI currently leads the DETER (Cyber Defense Technology Experimental Research) test bed effort for the U.S. Department of Homeland Security. Raytheon has sponsored research at USC-ISI on context-aware analysis for detecting social cybersignatures and social network analysis. This builds on USC's work in natural language processing and artificial intelligence. Some challenging problems ISI is tackling include:

- Detection and characterization of hidden actors and groups
- Techniques to model and discern social patterns, detect informal groups and roles of group members as they cluster around topics of interest, or detect when someone is talking "around" a subject
- The tracking of attitudes and levels of interest in a topic over time, and finding interesting patterns out of networks with more than one million nodes

ISI's research helps answer questions such as: Who is infiltrating? What are they looking for? Why are they doing this?

University of Illinois at Urbana-Champaign

The University of Illinois at Urbana-Champaign has established the Information Trust Institute, with more than 90 professors and staff exploring the challenges of critical infrastructure security. Through this partnership Raytheon can model and simulate the behaviors of the largest and most complex elements of critical infrastructure, including the public land mobile network, power systems and industrial control systems. With the university's Real-time Immersive Network Simulation Environment, it's possible to evaluate vulnerabilities of smart power grid architectures, predict performance of mobile applications over the national telephony network, and develop repeatable attack simulations.

Johns Hopkins University

Systems engineering provides the foundation for secure and reliable solutions to challenges in the cyberdomain and all others. Familiar systems engineering concepts such as risk management, independent testing, design validation and configuration control take on special importance within the world of cybersecurity engineering. Raytheon Engineering has partnered with Johns Hopkins University (JHU) to offer an onsite Master of Science in Systems Engineering degree program that began in January 2009. Its purpose is to assist students in developing the systems engineering knowledge, skills and tools necessary to successfully lead the planning, development and engineering of large, complex systems.

JHU was selected after a comprehensive eight-month study of national university programs, which considered the relevance of curricula, industry experience of instructors, the flexibility to incorporate Raytheon-specific content into curriculum, measures to encourage and simplify employee participation, and the university's reputation within our customer acquisition community. Raytheon's five-course certificate program comprises basic systems engineering courses with a capstone project. The master's degree requires five additional courses, among them several with value in cybersecurity: System of Systems Engineering, Systems Architecting, Management of Complex Systems, Modeling and Simulation in

Robert Batie (left), NCS senior principal engineer, talks with Andrew Tappert from Pikewerks at Raytheon's recent SBIR Industry Day event.

Systems Engineering and Advanced Technology.

Other Collaborative Relationships

Raytheon is participating in several other university partnerships.

- Penn State University will support Raytheon in developing software to represent target tracking and hyperbolic browsing in 3-D immersive visualization environments.
- Raytheon recently completed experiments with the University of Maryland's computer intrusion detection technologies. Their knowledge-based approach collects and analyzes information from some 40,000 campus computers to determine which are most likely compromised.
- Raytheon is working with researchers at the State University of New York at Buffalo to incorporate their Information Fusion Engine for Real-time Decision-making into a large-scale cyberrange. INFERD is designed to provide real-time situational awareness and decision support to improve an analyst's ability to cope with the volumes and data rates possible in cybersecurity.

Small Businesses

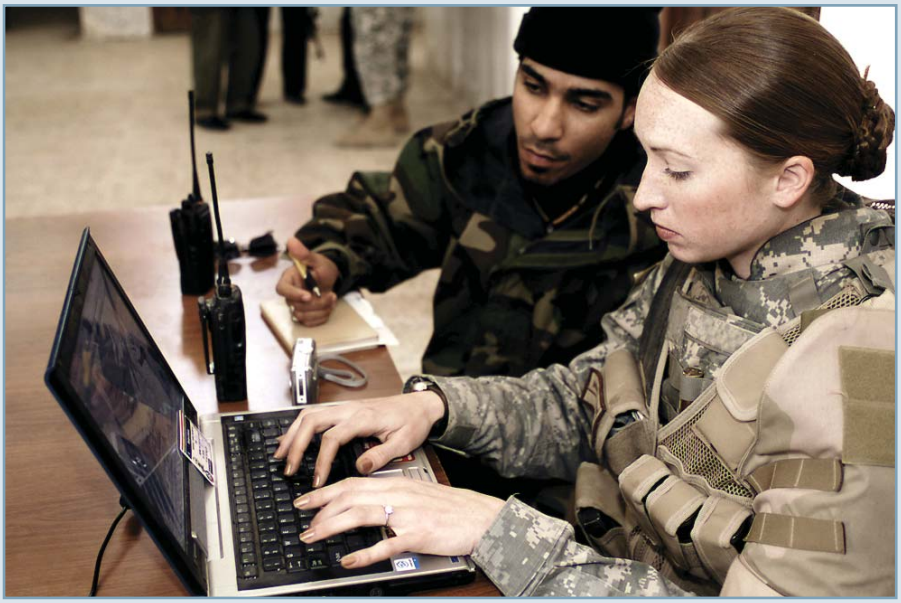
Some of the more promising and mature technologies are spun out of universities into small businesses. Many of these companies compete for part of $2 billion in funding designated annually by the federal government, and administered through the Small Business Administration in its Small Business Innovation Research and Small Business Technology Transfer programs.

Raytheon hosted an industry day event where 22 small businesses specializing in cyberdefense technologies came to hear from Raytheon and our customers. Individual one-on-one sessions allowed each company to meet with experts from around Raytheon who had an interest in the company's technology. These partnerships have resulted in many letters of endorsement and successful joint pursuits of follow-on research contracts from government science and technology customers. ●

Jon Goding
jgoding@raytheon.com

Enabling Information Sharing: Balancing Need to Know With Need to Share

Since Sept. 11, 2001, the traditional information security approach of restricting access to information has faced the challenge of balancing need to know with the necessity of sharing information to achieve Mission Assurance. Two demonstrations at the 2008 U.S. Department of Defense (DoD) Coalition Warrior Interoperability Demonstration (CWID) established Raytheon's commitment to providing state-of-the-art, secure, interoperable information sharing. The demonstrations also laid the groundwork for developing new collaboration systems for use in the field by U.S. and coalition partners.



New Information-Sharing Paradigm

The 9/11 Commission Report published in July 2004 recommended a network-based information-sharing system that transcends traditional government boundaries to unify the many agencies involved in countering terrorism. Our military faces a similar need-to-share challenge as it increasingly participates in combat operations with multinational partners. Coalition forces can gain an advantage by providing timely access to relevant data on the Global Information Grid (GIG), which is composed of tactical-edge networks and higher-echelon sanctuary networks, all of which need to securely interoperate with each other.

At the surface, it would appear that tactical networks require less protection than sanctuary networks. For example, the threat duration and the risks versus rewards of data sharing can be substantially different under the fog of war. Targeting data may be extremely sensitive during mission planning, but become news on CNN in a matter of minutes after mission execution. The risks associated with temporarily sharing classified data with coalition partners may be outweighed by the opportunity to enhance mission effectiveness and/or save lives. In contrast, the duration of the threat against sanctuary networks is measured in years.

Continued on page 34

Continued from page 33

Military networks can benefit from adaptive security policies that can flex to conditions and force composition, and incorporate the user's needs into the information-sharing decision — rather than relying solely on the pre-judgment of the data originator.

Compartmented High Assurance Information Network

In order to more quickly field emerging technologies that could meet the necessary criteria, the DoD established the CWID, an annual event that aims to engage cutting-edge information technology to enhance warfighter information-sharing capabilities. Each technology trial is evaluated using a scripted scenario involving coalition participation, and each receives focused feedback in terms of its user interface, operational utility, interoperability issues, and information assurance (IA).

In 2008, Raytheon demonstrated its Compartmented High Assurance Information Network (CHAIN) as a secure information-sharing solution at CWID. The 2008 scenario described notional coalition task force operations applicable to any global crisis, with scripted terrorist and natural-disaster events.

The need to quickly share information with the right partner at the right time is traditionally solved with stove-piped systems and "sneaker nets." CHAIN was designed to overcome stove pipes and provide a scalable, dynamic capability to support multinational operations.

CHAIN is a commercial-off-the-shelf-based security solution that allows for data sharing and collaboration between communities of interest and personnel of varying clearance levels, security caveats, and needs to know. It provides secure services such as e-mail, document control and collaboration, VTC, chat, and white-boarding. CHAIN also provides user-level authentication and role-based authorizations, along with the central management of security policies, which allows the system to quickly change security levels to adjust to the operational situation. Other security features include labeling and control of classified documents and e-mails, content validation, anti-virus protection, and data in-transit/at-rest protection.

At CWID 2008, CHAIN successfully provided a secure collaboration environment that exceeded the warfighter's expectations. Warfighters used CHAIN to coordinate missions, review intelligence data, and securely chat about current operations, as well as for mission planning (white-board function). While some warfighters were experienced computer users, several were not. Even in those cases, CHAIN's intuitive features (similar to the standard DoD desktop environment) enabled all users to quickly learn and use the IA features.

The CWID final report stated that CHAIN had met or exceeded warfighter objectives for secure coalition information-sharing, and rated CHAIN as one of the "most promising technologies." CHAIN is currently operational and is deployed to DARPA, accredited at Protection Level 3.

CHAIN laid the foundation for Raytheon's winning proposal submission for the Defense Information Systems Agency's Multinational Information Sharing (MNIS) Design, Transition and Operate (DTO) contract, valued at more than $135 million. Focused on providing enhanced secure collaboration networks for coalition operations, the MNIS DTO contract is the vehicle for developing and fielding new collaboration capabilities for our warfighters. MNIS will collapse existing coalition stove-piped networks into a single fabric enabled by CHAIN's IA services and features.

Trusted Enterprise Service Bus

Raytheon partnered with the World Wide Consortium of the Grid (W2COG) to help advance technology for dynamic security policy. The W2COG established a multinational-coalition scenario that required finding and engaging a covert maritime threat thought to be bringing ashore a weapon of mass destruction. Raytheon contributed a Web service for unmanned aerial vehicle sensor data. The capability allowed an occasionally connected UAV sensor suite to provide data via an open-source lightweight service bus to authorized users over the command and control (C2) network. The project successfully "flattened" coalition networks and enabled data and service discovery via semantic interoperability.

The team developed a prototype Web service stack designed to enhance information processing efficiency and to execute dynamic "protect versus share" security policies. The prototype was composed of a trusted enterprise service bus (T-ESB) at the server end, and a trusted C2 Web portal on the service-consumer end. In this case, trusted meant that T-ESB assured authentication and authorization at Protection Level 4 (PL-4). The Web service stack included PL-4 government-furnished authentication and authorization services, UAV sensor services, and intelligent software agents that provided a valued information at the right time service. The VIRT service issued a browser pop-up message when geospatially enabled software agents detected predefined critical conditions.

The server was deployed at Hanscom Air Force Base in Massachusetts, and provided all of the services used during the demonstration. The coalition watch officers deployed to various international sites. Using registered single sign-on credentials to authenticate, users consumed authorized Web services transparently via Microsoft Internet Explorer® and Mozilla Firefox® Web browsers.

Authorization depended on attributes, such as national identity, mission role and emergent situation.

At the beginning of the demonstration, each of the participants was issued sign-on credentials. Separately, a command authority predefined which information resources could be made available to which categories of consumers through a set of policies. The policies recognized several operational states (normal, emergency and self defense) and established different rules for each state. Participants accessed C2 resources through a Web site set up for the exercise. The Web site hosted authentication and authorization services, and governed user access based on the user's credentials and the policy for the prevailing operational situation.

Definitions of Operational Security Policies

As the trial scenario unfolded, intelligent software agents within the VIRT service looked for suspicious activity by monitoring ship tracks, meteorological and oceanographic (METOC) warnings, and UAV sensor data. If a ship's track data indicated a sudden course change, or a change with respect to national flag, or increased speed as it approached the three-mile limit of the U.S. West Coast, the VIRT service delivered a pop-up message to the appropriate watch officer's browser.

In response to this notification of an emergency situation, the watch officer immediately used a point-and-click menu to set emergency security policy. Because the situation demanded that non-U.S. coalition platforms interdict the threat, the policy authorized specific non-U.S. platforms to access the C2 portal to view local track and sensor data — data that would be withheld under normal conditions.

During the interdiction, intelligent software agents noticed a coalition interdiction platform in imminent danger of entering a mine field depicted on a SECRET NOFORN METOC warning. Accordingly, the VIRT service delivered a pop-up message. The alert triggered the U.S. national watch officer to authorize the endangered foreign vessel for self-defense level of access. When the interdicting vessel avoided the hazard and intercepted the threat vessel, the coalition watch officer reset the security policy to normal.

In a June 2008 memorandum titled "Role-player after-action comments and observations," CWID sponsor feedback on the demonstration was overwhelmingly positive. "Each time the security policy was set to a different level, all users whose operating-picture views were supposed to change did see the appropriately updated picture … The VIRT concept combines the best features of 'smart push' and 'demand pull' information management processes to provide probably the best shared, managed, situational awareness we can create right now … Helped forward the development of access controls."

A logical next step was to test the capability with live data feeds — a test that took place in late February 2009 at the Naval Postgraduate School–SOCOM Exercise at Camp Roberts, Calif. The team successfully executed a follow-on experiment using Raytheon's Cobra UAV to demonstrate dynamic access control of the UAV's full-motion video. As before, the dynamic policy engine provided secure authorization of network services based on user-provided, preapproved credentials, and successfully demonstrated emerging access-control technology.

The W2COG and Raytheon demonstrated their commitment and know-how to provide combatant commanders with state-of-the-art, secure, interoperable coalition data sharing. ●

Jerry Pippins
jerry_l_pippins@ raytheon.com
Contributors: David Minton, Paul Barré

Partnering with George Mason University on Secure Information Systems Research

Raytheon is working with researchers at George Mason University's (GMU) Center for Secure Information Systems to improve its ability to develop high-assurance systems. Current research and development activities include automating vulnerability analysis and hardening systems through secure virtualization.

Automating vulnerability analysis

CAULDRON (Combinatorial Analysis Utilizing Logical Dependencies Residing on Networks) is a tool that GMU recently developed to automate vulnerability analysis, the task of examining network security to identify deficiencies and predict the effectiveness of proposed improvements. Vulnerability analysis is performed manually today. To perform this analysis, engineers must find the vulnerabilities that an attacker could exploit and the many paths that an attack could take in order to traverse a network and reach the attacker's target. This has become an intractable task, as systems and networks have grown more complex and as exploits have become more numerous. Given thousands of exploits, vulnerabilities and possible network configurations, vulnerability analysis needs to be automated.

An attack may penetrate a network at one node and then hop from that node to reach a target at a remote node in the network. A multistage attack may employ different exploits along the way, as different nodes may have different vulnerabilities. It may also traverse the network via many possible attack

Continued on page 36

Continued from page 35

paths. A vulnerability analysis should ideally identify all possible attack paths, and the exploits and vulnerabilities used to traverse them.

Once the attack paths and exploits are known, developers may add security mechanisms or reconfigure the network in order to "harden" the network. Proposed changes can then be analyzed to predict their effectiveness before they are implemented. Multiple solutions can be explored at minimal cost if the process is automated.

Vulnerability analysis needs to be a continuing activity. Networks are dynamic places: they expand and are upgraded; new vulnerabilities are discovered, and so are new exploits. Each of these changes can affect the security posture of a network. By automating vulnerability analysis, CAULDRON makes it practical to periodically perform thorough vulnerability analyses, and find and eliminate new vulnerabilities before an attacker finds and exploits them.

Figure 1 shows CAULDRON's inputs. Commercial off-the-shelf tools provide information about network topology, known threats and intrusions. The user provides CAULDRON with attack scenarios that identify an attacker's potential network entry point(s) and target(s). CAULDRON then

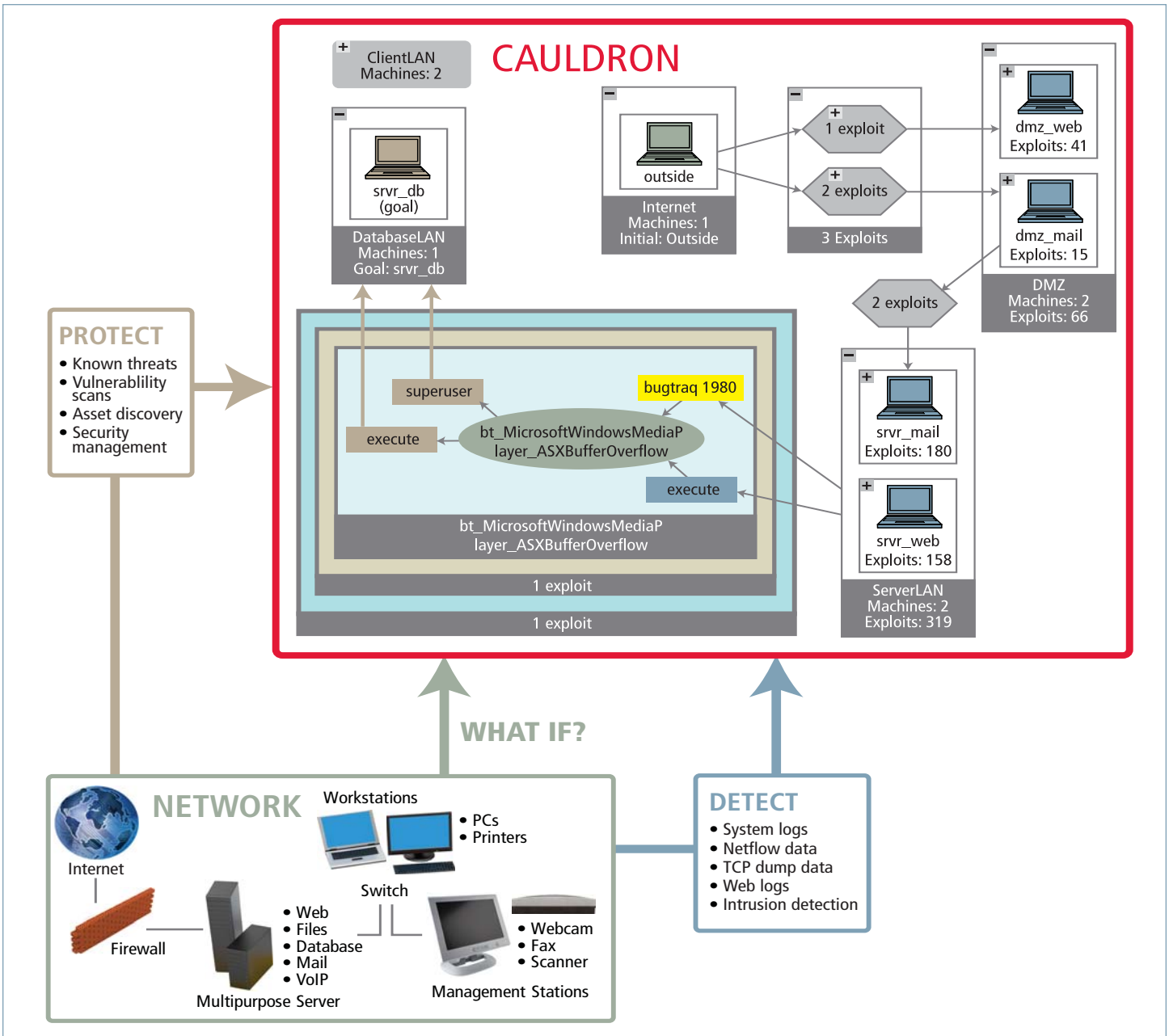


Figure 1. Inputs to CAULDRON

finds all of the paths and exploits that an attacker could use to reach those targets.

CAULDRON provides the user with visualizations of its analysis results, as shown in Figure 2. This gives the user information about attack paths, vulnerabilities, and exploits used, as well as recommendations for how network security can be effectively improved with minimal addition of security mechanisms. Raytheon has successfully used a beta version of CAULDRON on multiple engineering programs, both to evaluate its performance and perform vulnerability analysis.

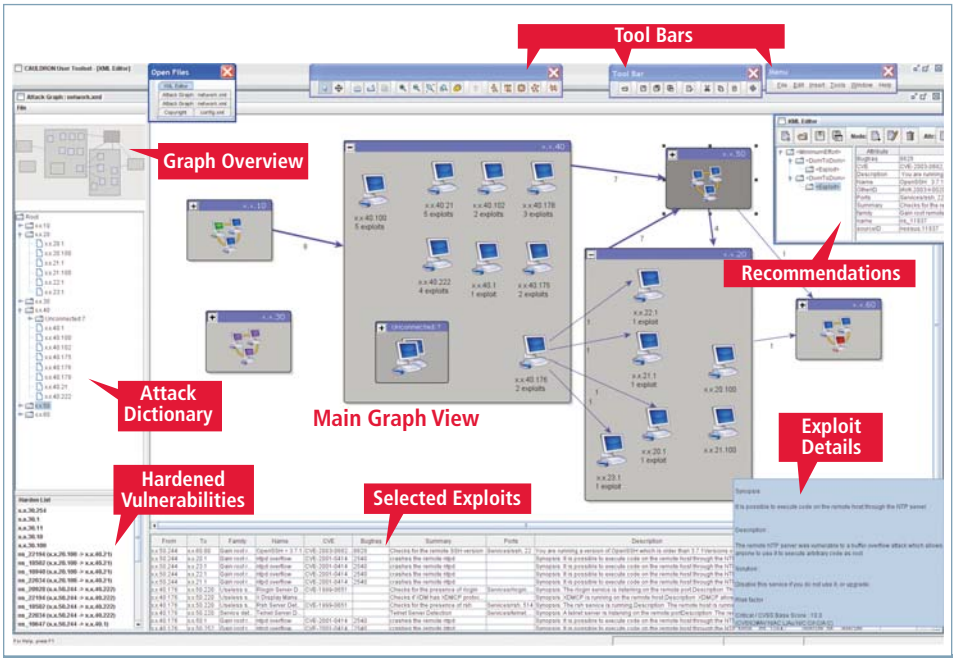


Figure 2. Visualization of Results

On one of these programs, an 81-host system with more than 2,300 open Internet ports was analyzed for vulnerabilities. Current practice would have required engineers to manually interpret vulnerability scan data, find critical attack paths and eliminate critical vulnerabilities. This would have taken weeks to do. CAULDRON found the attack paths, identified the critical exploits, recommended solutions, and helped eliminate 75 percent of the vulnerabilities in a few hours. The technology is being transitioned into Raytheon for further use as the technology matures.

Security Through Virtualization

Recent research has shown that virtual machines can be used to improve system security. The concept of a virtual machine has been around for many decades; it is a software implementation of a computer that executes a program like a real machine. For example, an application that runs on one operating system could also run on another operating system if a virtual machine were installed between the application and the second operating system. Security mechanisms can be combined with virtual machine technology to isolate a host computer from its applications in such a way that if an application is compromised, the application and its operating environment can be dismissed without harming the host computer or other applications.

Internet Cleanroom is one such technology. It protects hosts from Web-based attacks by running a browser or e-mail application on a virtual machine with mechanisms to detect and respond to compromise. Developed at GMU, it is transitioning into a commercial product offered by Secure Command. Raytheon is evaluating Internet Cleanroom for potential deployment in its own products and IT system.

The Uninterruptible Server is another technology that GMU is developing to protect servers from attack. It helps make servers intrusion tolerant, i.e., able to operate through an attack, even when the attacker has penetrated the system. The Uninterruptible Server runs multiple copies of server software on separate virtual machines, which are software emulations of the computers that run on real computers. As shown in Figure 3, each virtual server handles Internet service requests. A VS handler monitors each VS and makes local decisions to kill unauthorized processes that may appear due to Web-based attacks. Global decisions such as reverting servers are made by a trustworthy controller. A load balancer advertises a single IP address to the Internet and feeds Internet requests to the servers at random. The trustworthy controller is not addressable from the Internet side of the servers, so it is protected from Web-based attack.

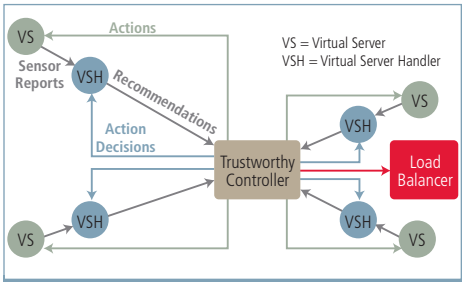


Figure 3. Uninterruptible Server

Raytheon is working with GMU to adapt these technologies for use in Raytheon systems.

Tom Bracewell
bracewell@raytheon.com

Lynn Dugle
President
Intelligence and Information Systems

Lynn Dugle is a Raytheon Company vice president and president of Raytheon Intelligence and Information Systems (IIS). She assumed leadership of IIS in January 2009, having previously served as vice president and deputy general manager of that business. Prior to that, she was vice president of Engineering, Technology and Quality for Raytheon Network Centric Systems. Dugle came from the commercial world before joining Raytheon in 2004, holding officer-level positions with ADC Telecommunications and positions including vice president of quality for the Defense Systems and Electronics Group at Texas Instruments. She started her career as a manufacturing engineer.

Technology Today recently caught up with Dugle at IIS headquarters in Garland, Texas, to talk about her new role and the big opportunities for Raytheon, including cybersecurity.

TT: *You recently became president of the IIS business at Raytheon. What are your top priorities?*

LD: Growing our business. It is absolutely clear to me that the key to growth is our ability to (1) apply leading-edge technologies to solve our customers' hardest problems, (2) team with companies and universities who are best in their class, and (3) hire creative, passionate people who want to run fast.

TT: *When you think about the future business and opportunities ahead, what do you see?*

LD: I see the future playing out a movie on fast forward — in which the threat and defense moves occur literally at cyberspeed. In the intelligence business, our adversaries have access to many of the same commercial technologies, so staying ahead of them requires us to rapidly recognize the potential of emerging innovations and, even more rapidly, to mash the right technologies together. We have to be aware, creative and fast.

When you look at the technologies that are driving our business, the list reads like the table of contents in the latest edition of "Wired" magazine. This is a very exciting time to be working in this industry.

TT: *I see you have a diverse background with non-traditional defense experience. How is your background helping in your position as president of IIS? Do you see a difference between the various industries managing data on huge networks?*

LD: I'm a big believer that different perspectives bring better solutions, especially in a business like ours where it's all about innovation and speed. On a personal level, I worked in the telecom industry during a time of amazing change, and I experienced firsthand the importance of making decisions quickly and moving forward at the speed of innovation. Otherwise, the market will unquestionably pass you by. My experience in telecom also made me very comfortable moving into new and unfamiliar territory, which is extremely important as IIS aggressively tackles the challenges of cyber, homeland defense and border security, just to mention a few of our key growth areas.

TT: *What are Raytheon's plans for the cybersecurity market?*

LD: Cybersecurity is one of the most extraordinary challenges of the 21st century. The threat of cyberattacks lurks behind every device we and our customers use to operate in our network-enabled world. Everything is vulnerable to attack. To face this challenge requires an entirely new mindset that is not timid about enlisting and fostering the nation's top talent, working at the extreme scale, and shattering traditional defense models. While the full suite of our cybercapabilities is not widely publicized, it is unprecedented. Our core competencies span everything from customer analytics and information assurance — leaving no doubt about the authenticity and security of the system we are delivering — to the far leading edge of the information operations frontier.

We are leveraging our extensive experience with the nation's most demanding cyber challenges and creating architectures and systems that anticipate the next threat well above the level of fighting the daily battle for cybersecurity. To be the best defender, you have to understand the tools of the best attackers.

TT: *What are Raytheon's capabilities in cybersecurity?*

LD: Simply put: Cyber is in our DNA. While we don't talk openly about our capabilities, we agree with the adage, "If a system ever had, has, or will have electrons or photons flowing through it, it is vulnerable." In other words, wherever information is generated, sent or stored there are vulnerabilities that create risk and opportunity for our business. We are quite fortunate to have a diverse team of scientists and engineers who truly understand the various depths of these statements and are committed to addressing our customer's toughest cybersecurity challenges.

Our capabilities span both the offensive and defensive side of cybersecurity, which is a unique proposition in the marketplace. In addition, during the last couple of years, Raytheon has added to its strong internal cyber credentials with the acquisition of three highly capable companies. Each brings several significant capabilities to allow Raytheon to respond to the full spectrum of cyber challenges. For example, Raytheon Oakley brings strong insider threat products and services that protect government and commercial networks from the inside out.

It is the fusion of these capabilities that allows our business to address cyber-related demands at multiple levels, from the device to the enterprise, from the small closed network to the global network community. Our layered approach enables Raytheon to tailor our solutions for the wide range of systems that customers operate.

TT: *Since 9/11, we've heard a lot about data sharing and interoperability. What is Raytheon doing in this regard?*

LD: Data sharing is a monumental problem that continues to plague our customers, bringing with it considerable expense and significant mission impact. Part of our strategy in IIS is to provide customers with "collect anywhere, exploit anywhere systems." This means that, irrespective of whether data is collected via satellite, UAV, human agent, robot, cell tower, etc., that information can be available to any authorized user anywhere in the world in very near real-time. A great example of sharing and interoperability is our recently completed capability to deliver information instantaneously to the warfighter on a device leveraging the Google™ Android mobile platform. Our biggest challenge will be extracting usable information at speed, at scale.

TT: *We hear a lot about cyberprofessionals. What exactly is a cyberprofessional?*

LD: Cyberprofessionals are engineers who have specialized knowledge in computer system internals, network security and data integrity. They bring a hacker's passion and creativity to understanding how systems are put together and where the vulnerabilities are. These are the engineers who take on our adversaries in cyberspace, and they have the ability to play offense as well as defense.

This is a very exciting part of our business and an area that will undoubtedly bring future growth, not only in the defense industry, but in other areas of technology. If I were in the early- or mid-career stage, I would think very seriously about developing my cyberskills.

TT: *What is Raytheon doing to help get more students to pursue math and science careers?*

LD: It's vital to get students hooked on math and science when they're young. Raytheon is encouraging interest in science, technology, engineering and math careers through initiatives to coach, fund and engage students who have the promise to be future engineers.

We actively promote math and science education for younger students through activities such as our innovative MathMovesU® program. Raytheon is also a title sponsor for the 2009–2011 MATHCOUNTS® national competition, and we provide numerous scholarships. We also sponsor many local and statewide robotics competitions each year.

TT: *What advice do you have for young engineers entering the field?*

LD: Follow your passion and have fun! Which I, of course, assume will bring you to Raytheon. It's an exciting place to be. We're hiring — everything from sensor physicists to detect single photons in outer space, to cyberwarriors to protect exabytes in cyberspace. Raytheon has a position for those with a career calling to keep our nation and our allies safe through leading-edge technology. ●

MEET A NEW RAYTHEON LEADER

One of the newest members of Raytheon's cyberdomain team is ***Randall Fort, director of Programs Security.*** *Fort joined Raytheon after nearly 30 years of protecting the United States' interests through security and intelligence leadership roles in both the public and private sectors. He was most recently the assistant secretary of state for Intelligence and Research.*

In November 2009, he became the fourth recipient of the National Intelligence Distinguished Public Service Medal, the highest award granted to non-career federal employees, private citizens or others who have performed distinguished service of exceptional significance to the intelligence community.

"Technology Today" caught up with Fort to discuss his current and past roles, and the customer's perspective on the cyberdomain.

1. What did you do at the Department of State?

I was the assistant secretary of state for Intelligence and Research, and I headed the Bureau of Intelligence and Research, or INR, the oldest civilian entity in the U.S. Intelligence Community. There were four key roles: First, I managed the production of all-source intelligence analysis and the dissemination of that information to the Secretary of State and other senior policy-makers. Second, we coordinated U.S. intelligence operations to ensure compatibility with U.S. foreign policy. Third, INR was the center of the government's unclassified overseas public opinion polling and media analysis. And finally, I served as chairman of the Cyber Policy Group, coordinating all aspects of the department's engagement with cyber policy and operations.

2. How did you come to be involved in cyberspace issues?

Very early in my tenure, I encountered several significant cyber issues, and began asking questions about how the department was managing its foreign policy and diplomatic responsibilities in cyberspace. What I discovered was a lack of awareness, focus and understanding of cyber-related issues. Because of my persistence and interest in the issue, the secretary asked me to conduct a review of the department's cyberspace policy, resources and authorities in the summer of 2007. Coincidently, that was the same time that the Director of National Intelligence was leading a cybersecurity review, which led to the Comprehensive National Cybersecurity Initiative (CNCI) later that fall. Our review, which identified for the first time who was working on cyber, how much we were spending, and with what authorities, recommended the establishment of a department-wide coordinating group to manage cyber internally and represent State in the interagency process on cyber issues. The secretary accepted our recommendations and appointed me to chair the new Cyber Policy Group, a role I fulfilled for two years.

3. What do you think is the government's biggest cyber challenge?

This may sound odd, but I believe their biggest challenge is to adopt a new way of thinking. Cyber is not a conventional issue — it defies the typical two-dimensional organization charts, bureaucratic stovepipes, and traditional missions. It cuts across and touches almost every area of government activity, so there is no natural or single leader.

4. What does customer success look like in cybersecurity?

First, the customer, especially the government, needs to be clear about what they are seeking. Are the solutions just for local or proprietary systems, or should they be applicable and/or scalable to broader systems and networks? Ultimately, cybersecurity must be an inherent part of any technology product or system that is a part of the global network. It can't be an afterthought or add-on to our technology; rather, it must be incorporated from the beginning.

5. Since you were part of the senior intelligence community leadership, what were your most difficult challenges?

Integrating the IC under the auspices of the new Director of National Intelligence leadership structure was one significant issue that confronted every agency in the community. Second, supporting our military forces and diplomatic officials in the field engaged in two major military conflicts was a daily concern, especially since so many lives were at risk. Third, in addition to dealing with all of the daily, current issues and threats, we were confronted with a rapid rate of technological change, and the attendant challenges of managing

all the consequences of that change, from hiring and retaining the right workforce, to developing and adopting the right set of tools and systems. Fourth, and following the last point, the IC struggled to deal with the exponential growth of so-called "open source" intelligence — today, vast quantities of statistical data, satellite imagery, and other information are unclassified and relatively easily available to anyone with the time and tools to discover it, creating competition for the IC. Lastly we were dealing with a major change in strategic outlook: In the Cold War, the IC focused on collecting, processing, analyzing and disseminating intelligence on the so-called "denied areas" of the Soviet Union and its allies, a geographically confined and politically defined area. The IC was structured around the intelligence challenge posed by that target. Today, the IC is challenged to target "denied minds"; that is, hostile individuals, such as the al-Qaeda leadership, who may be located anywhere, communicating with anyone at any time. We've gone from trying to find a needle in a haystack, to trying to find a specific needle in a stack of needles. And our organization and strategy have not evolved sufficiently to address those new, dynamic threats.

6. Director of Programs Security is a new position at Raytheon — what are your chief responsibilities?

Let's take a step back: Security has traditionally been managed in functional silos, such as physical security and access control, personnel or information technology. Those distinctions were traditionally appropriate, but are no longer sufficient to ensure effective security. The existence of numerous special access programs, or SAPs, at Raytheon with separate, overlapping and sometimes confusing requirements is another complicating factor. My role will be to work with the businesses to integrate our security functions across the spectrum of activities. Also, I will work within the security community and our government partners to develop security standards and practices that leverage modern technology and tools to address real threats and challenges. Ideally, security will be a strategic enabler, not an impediment, to the safe and efficient conduct of our business.

Another of my roles is to provide executive leadership for the Raytheon Cyber Tactics Center, a cyber range capability that Raytheon is deploying as a common engineering tool across the enterprise. The RCTC provides an engineering environment for the integration of Raytheon-wide cybersecurity capabilities. It also allows us to evaluate embedded cybersecurity and protection across the broad range of C3I, sensing, effects, homeland security and other systems and solutions that Raytheon provides to our customers.

The RCTC will provide a secure facility for hardware and software testing as well as a learning facility for Raytheon engineers, customers, and industry and academic partners. Its capabilities will allow us to more effectively leverage the capabilities of government cyber ranges that are planned or in development, such as the DARPA-sponsored National Cyber Range (on which Raytheon BBN Technologies is teamed with Johns Hopkins APL for the Phase II contract).

7. How have your prior experiences help prepare you for this role?

I've served in the U.S. government for more than 15 years of my career, so I have a good understanding of the government's perspectives and requirements. I've been involved in the intelligence business for 27 years, either directly as a government employee or indirectly as a contractor or advisor, and so I have considerable background and experience in the security requirements and measures surrounding sensitive and classified programs. In fact, as the Senior Official of the Intelligence Community at the State Department, I controlled access to all code-word level intelligence for the entire department. Finally, as director of Global Security at Goldman Sachs, I was responsible for all aspects of physical security and crisis management.

8. How can security contribute to implementing our strategy and executing our business?

If our people are our most important asset, then assuring that they work in a safe and secure environment, able to perform their jobs without distraction from external threats or dangers, is the highest security priority. Security must be a partner with our businesses and employees, supporting and enabling the successful execution of our commitments. It should not be an obstacle or unnecessary burden to achieving results. The government sometimes imposes overlapping, onerous security requirements, and we need to work within the security community to rationalize and modernize those requirements and leverage new technologies to achieve appropriate security outcomes in less time and at lower cost. Improving security efficiency and effectiveness will have positive impacts on all Raytheon businesses.

9. Coming from the outside, what are your first impressions of Raytheon?

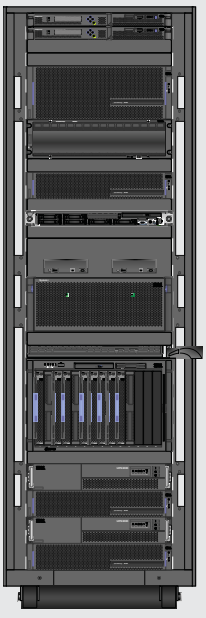
First, the people here are extraordinary: extremely smart, focused, enthusiastic about their work, and very open and welcoming to me as a new member of the team. Second, I am truly dazzled by the sophistication and breadth of the technologies I am encountering during my travels around the company — nearly science fiction-type capabilities are seemingly routine, and I know I've just scratched the surface so far. Third, I am deeply impressed by Raytheon's history and the depth of its culture; for example, the seminal role the company played in the Apollo moon landings was a fascinating case study highlighting our technical accomplishments. Last, Raytheon is a big company with many operating units widely dispersed; integrating and coordinating all those capabilities during a time of rapid technology change will be a major management challenge going forward. ●

RedWolf™

Mission-Driven Technology Advancement

The name *RedWolf* may not be well known to the public, but it is known and highly respected by agencies tasked to protect the U.S. homeland and perform other lawful surveillance functions.

The engineers and managers of the Telecommunications Surveillance Products (TSP) program, part of Raytheon's Intelligence and Information Systems business, have directly supported the missions of their criminal investigation community customers for over a decade. These developers of the RedWolf product line of audio and electronic data surveillance systems often work on site with customers to ensure the peak performance of operational systems, as well as to derive requirements for the continued enhancement of RedWolf products. This on-site presence can lead to challenging assignments for the RedWolf development team, whose members were on the ground in New York City just days following the Sept. 11, 2001 terrorist attacks.



A RedWolf large system can scale up to accommodate hundreds of law enforcement users.

RedWolf's primary customers are national-level government agencies that perform court-warranted surveillance — such as the FBI, the Drug Enforcement Administration and similar organizations in other countries. Hands-on support of these customers drives the technical evolution of the RedWolf product line.

Originally developed to support simple telephony and audio surveillance, RedWolf has been expanded in recent years to include direct integration with wireless telephone service providers and a comprehensive Internet traffic collection capability. This expansion requires RedWolf engineers to react quickly to the ever-changing and expanding technology used by telecommunications service providers and the multitude of available online services. This fast-reaction system revision capability is facilitated by the open-architecture development approach that has been a hallmark of the RedWolf system architecture since its inception.

Evolving customer needs continue to push RedWolf toward new capabilities and technical advances. As RedWolf systems have grown in size and technical capability, and customer missions have become increasingly focused on criminal intelligence, users have requested analytic tool enhancements. In response to this need, within the past year the RedWolf team has integrated a number of new capabilities, including a secure text search feature that enforces essential data access restrictions; automated mapping of cellular telephone system location reports; and automated voice processing for speaker identification, plus language and gender recognition. Work has begun on integrated link analysis tools and databases to support investigation of social networks. These tools will soon be available.

TSP engineers are particularly enthusiastic about a 2008 exploratory study of the automated voice identification and recognition capability. Initial results have been very promising. TSP chief engineer Art Stefanelli explained the primary concept supporting the addition of this capability: "Intercept operators must try to [determine] the exact identity of the person(s) who are speaking to the surveillance target during a call that is pertinent to the investigation. The voice processing system should help them make this determination more quickly and accurately by showing voice matches against a set of previously identified associates for which good speech samples exist."

RedWolf engineers are keenly aware that a hyper-efficient development timeline is important to customers in the high-stress criminal investigation community. Therefore, RedWolf's development and marketing approach has been revised to reflect the unique needs of these customers, who do not tend to invest in long-term custom-built development projects. Instead, they demand capabilities offered as off-the-shelf products — products that can be quickly customized and installed within an operational environment with minimal disruption of the day-to-day mission. This product line development and sales approach, which departs from the traditional custom-development business approach of many Raytheon programs, may well be as innovative as the technology advancements that characterize RedWolf's evolution.

Despite the success of the 2008 research, RedWolf engineers are not content to rest; further technology advancements are already on the drawing board. As the customer mission evolves, RedWolf will also evolve as part of TSP's firm commitment to support that mission. The need to integrate sophisticated analysis capabilities across multiple systems is driving RedWolf developers to adapt more of the available analytic technology from the intelligence community to the lawful surveillance community. It is expected that other drivers of future capabilities will stem from the complex statutory guidelines that RedWolf customers follow. These guidelines, which can include important and far-reaching regulations like the USA PATRIOT Act, are the result of an increasing cognizance of privacy issues related to the capture, processing and retention of personal data.

Based on their stellar record of mission support to their customers, we believe that TSP's engineers are well equipped to meet the new challenges that the future will undoubtedly bring. ●

Jeanne Minahan Robinson
jrobinson@raytheon.com
Contributor: Art Stefanelli

Cyberspace 101: Internet Basics

The Web is increasingly important to Raytheon's customers and businesses. Now, with Web-based applications being posed as an alternative to PC-based applications, and with cloud computing potentially enabling entire computer services to be outsourced, this might be a good time to remind readers of some Internet basics.

How Did It Develop?

The concept of the Internet — using packet switching rather than circuit switching — came from a study done for the U.S. Air Force to create a highly robust, survivable network. BBN Technologies was awarded the Air Force contract in April 1969.[1] Breaking data into packets enables more efficient use of a shared circuit, and improves robustness because each packet's arrival at a destination can be confirmed. When failure occurs, a missing or corrupt packet can be re-sent to ensure successful reception. Because packets can take different routes to a destination, a packet-switched network can overcome data congestion by routing packets around "traffic jams." This ability to determine different routes for packets to follow enables the network to survive loss of physical circuits without interruption.

Although several packet-switched networking solutions were developed in the late 1960s and 1970s, most could not communicate with each other because they used different proprietary protocols. Developing a simple common network system — Transmission Control Protocol, Internet Protocol (TCP/IP) — separated the concept of the network from its physical implementation.

When the Advanced Research Projects Agency Network was interlinked with the National Science Foundation Network in the late 1980s, the term *Internet* was coined to describe a large, global TCP/IP network. The old external gateway protocol was later replaced by the border gateway protocol (BGP), allowing the removal of the NSFNet Internet backbone network. The BGP is the core routing protocol of the Internet and makes data routing decisions based on path, network policies, and rules sets. This approach abandoned the single-core architecture of NSFNet and turned the Internet into a meshed infrastructure, with fully decentralizing routing.

In 1994, classless interdomain routing (CIDR) was introduced to better conserve address space, decreasing search times, and to permit route aggregation that decreased the size of routing tables. This approach supports addresses specified in CIDR notation, which allows blocks of addresses to be grouped into single routing table entries known as CIDR blocks.

What Are the Major Internet Components?

The Internet consists of computers interconnected with routers. Routers are networking devices that route/forward information, connect two or more logical networks (subnets), manage traffic, and bound subnets. Subnetting is used to break the network into smaller, more efficient networks, thereby preventing excessive packet collisions that would result in those packets being resent. Subnetting is independent of the network's physical layout and leverages the fact that most devices have more than one logical address, though only one physical address. Multiple logical addresses facilitate hardware switchovers when a component fails.

What Are Packets and Datagrams?

The information passed through the routers is in *packets*, which are data units containing user data (the information being transported) and control information (information the network needs to deliver the user data). *Packet* applies to units of data in a "reliable" service; i.e., one that notifies the user when the delivery fails (such as TCP/IP). *Datagram* applies to units of data in an "unreliable" service such as User Datagram Protocol/Internet Protocol

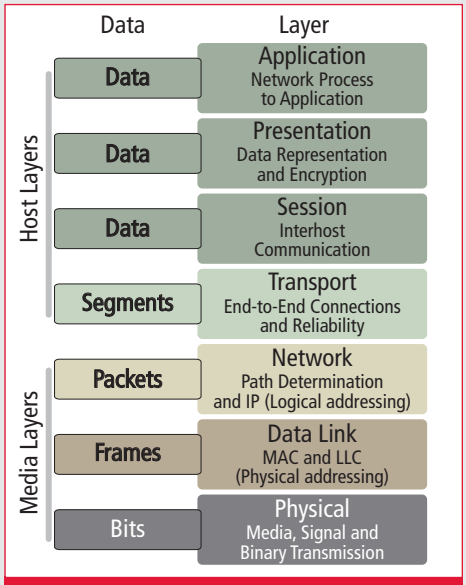


Figure 1. The Open Systems Interconnection Reference Model shows the hierarchy used by the Internet to communicate.

(UDP/IP). TCP and UDP are the best examples of mechanisms for the transport layer, layer 4 of the seven-layer Open Systems Interconnection Reference (OSI) Model. Packets and datagrams have a common structure consisting of a *payload* (the bits of data you are trying to get from here to there); a *header* identifying source and destination; and other information needed to interpret the datagram, apply quality of service, and reassemble the series of payload blocks into a coherent stream at the destination. Moreover, packets are nested: An IP datagram with its header indicating source and destination IP address may carry a payload that is itself a TCP packet with its own header, enabling simultaneous streams, or "sessions," between the two addresses to be kept separate.

An important aside: The openness and diversity of traffic in an IP network can make it difficult to enforce security. In an innovative move to address the challenges of network security, Raytheon has formed a

Continued on page 44

Continued from page 43

partnership with Narus, the leader in real-time traffic intelligence for the protection and management of large IP networks, in which Raytheon will embed NarusInsight™ to monitor IP traffic and provide critical knowledge to help manage and protect sensitive government networks.

What Are Open Systems Interconnection Reference (OSI) Model Layers?

Each OSI layer is a collection of similar functions that provide services to the layer above it and receive services from the layer below it. For example, a layer that provides error-free communication across a network furnishes the path needed by applications above it and calls the next-lower layer to send and receive packets containing the data contents.

A major division is made between the lower four OSI layers and the three upper layers (see Figure 1). The first three OSI model layers — the physical layer, data link layer and network layer — enable network functions to move data from one place to another. The physical layer moves bits over wires, the data link layer moves frames (a digital data transmission unit containing a link-layer header followed by a packet) on the network, and the network layer moves packets/datagrams over the network. The transport layer, in the middle of the OSI model, is the transition point between the hardware-associated layers below and the more software oriented, abstract layers above. The transport layer bridges the higher-layer applications (which send data reliably without error correction, lost data or flow management) with network-layer protocols (which are often unreliable and unacknowledged). The upper layers provide user interaction and implement software applications, protocols and services that let us actually use the network. Although the upper layers are harder to separate from each other because many technologies and applications implement more than one of layers 5 though 7, this is not important; the TCP/IP suite lumps these higher layers together.

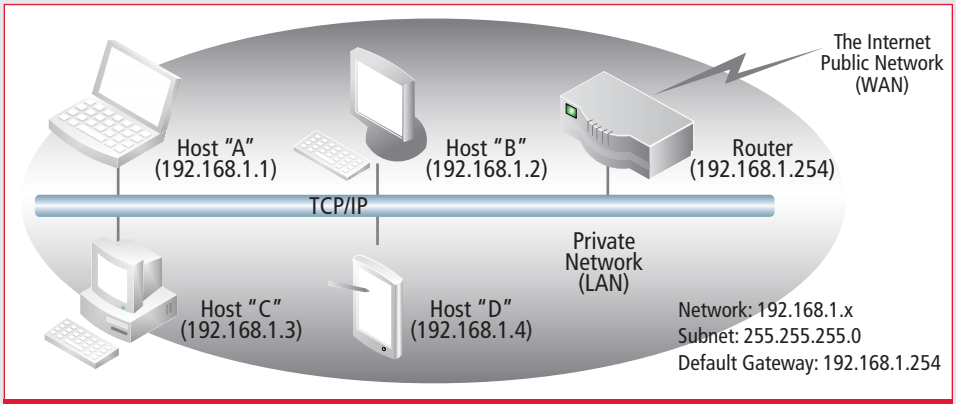


Figure 2. All communication is via the router, and private networks are hidden from direct public network (also known as wide area network [WAN]) access.

How Are Packets/Datagrams Transported?

To transport packets, the router must know their sources and destinations. IP addresses identify a device connected to a particular network and are used for communication between nodes. IPv4, the dominant Internet Protocol version, has 32-bit addresses following *000.000.000.000* format. IPv6, the latest version, has 128-bit addresses following *000:000:000:000:000:000* format. An IP address is divided into a network address and a host identifier. The subnet mask (in IPv4 only) or the CIDR determines how the IP address is divided into the network as host parts.

A computer can be configured to use the same IP (static) address each time it powers up or a different (dynamic) address each time. Dynamic IP addresses are most frequently assigned on local area networks (LANs) and broadband networks by Dynamic Host Configuration Protocol (DHCP) servers. Using dynamic addresses avoids the administrative burden of assigning specific static addresses to each device on a network and allows many devices to share limited address space on a network if only some of them will be online simultaneously. Most current desktop operating systems use dynamic IP configuration by default so that a user need not manually enter settings to connect to a network.

What Is Network Address Translation?

Because the IPv4 format's limited number of Internet addresses would not easily handle the world's growing number of Internet users (now more than 1.6 billion), network address translation (NAT) devices/firewalls became an indispensable feature in routers for homes and small businesses. Most systems using NAT enable multiple hosts on a private network to access the Internet through a single public IP address. NAT breaks the originally envisioned model of IP end-to-end connectivity across the Internet, complicating communication between hosts and impacting performance. NAT obscures an internal network's structure, creating a single "public" address that shields the network's "private" addresses so that all traffic appears to outside parties to originate from the gateway machine (see Figure 2).

Network address translation involves rewriting the source and/or destination IP addresses and usually also the TCP/UDP port numbers of IP packets as they pass through the NAT. Checksums (both IP and TCP/UDP) must also be rewritten to account for the changes. Typically, a local network uses one of the designated private IP address subnets. Private network addresses are *192.168.x.x, 172.16.x.x* through *172.31.x.x*, and *10.x.x.x* (CIDR notation: *192.168/16, 172.16/12,* and *10/8*), and a router on that network has a private address (such as *192.168.0.1*) in that address space. The router is also connected to the Internet with a single "public" IP address (known as "overloaded" NAT) or multiple "public" addresses assigned by an Internet service provider.

As traffic passes from the local network to the Internet, each packet's source address is

translated from the private addresses to the public address(es). The router tracks basic data about each active connection (particularly the destination address and port). When a reply returns to the router, it uses the connection tracking data it stored during the outbound phase to determine where on the internal network to forward the reply. The TCP or UDP client port numbers are used to demultiplex the packets when NAT is overloaded. On packet return, the IP address and port number are used when multiple public addresses are available. To a system on the Internet, the router itself appears to be the traffic's source/destination.

IPv6 provides a much larger (128-bit) address space than IPv4's 32-bit addresses, allowing for an astronomically high number of addresses. The expansion provides flexibility in allocating addresses and routing traffic and somewhat eliminates the need for NAT devices/firewalls. (NAT will probably be retained in legacy private networks because of the redesign work required to remove it.)

NAT limits the demand for IPv4 addresses but lacks network security.[2] IPv6 includes network security in the form of Internet Protocol Security (IPSec). IPSec is used in some IPv4 networks, but it is a requirement in IPv6 networks. It is widely expected that IPv4 will be supported alongside IPv6 for the near future. IPv4-only nodes cannot communicate directly with IPv6 nodes and will need assistance from intermediary dual-stack hosts.

Conclusion

The Internet continues to offer business opportunities and challenges, and we must be proactive in understanding and dealing with both. Our customers deserve no less. ●

Donna M. Czysz-McConnell
donna.czysz-mcconnell@raytheon.com

[1]BBN Technologies was recently purchased by Raytheon and is now Raytheon BBN Technologies, a part of the Network Centric Systems business.

[2]For more information about IPv6 and cybersecurity, see Information Assurance for Communication Systems, also in this issue.

Mission Systems Integration Technology Network Symposium

Raytheon's Technology Networks symposia are some of the most successful sources of knowledge exchange and employee networking available to the engineering communities at Raytheon Company. The Mission Systems Integration Technology Network (MSITN) continued this success at its 2009 symposium held Aug. 10–13 at the Westin La Paloma in Tucson, Ariz.

With the theme, "From Mission Need to Customer Success," the symposium addressed the system life cycle from customer mission understanding, through integration and validation, to deployment and operational support. The MSI Technology Network is the champion of technology and knowledge that enables Raytheon to act as the customers' agent in achieving their missions. Its role is to promote the exchange of relevant knowledge, technology and best practices across Raytheon.

Mission-Based Solutions

The 2009 symposium began with its first plenary speaker, Dr. Taylor W. Lawrence, Raytheon vice president and president of the company's Missile Systems (MS) business.

"Raytheon's Mission Systems Integration expertise provides our company with the opportunity to combine its vast array of products and services to give the warfighter a single, seamless, mission-based solution," Lawrence said.

"Our unique ability to integrate critical mission systems is in high demand worldwide, a demand that will only increase as we grow globally. Through MSI, we are able to better share innovations across the company and partner with our user community and world-class suppliers, to net solutions together for customer success. This further reinforces Raytheon's commitment to no doubt Mission Assurance," he added.

Other keynote speakers included:

- Barbara Johnson, vice president of Ground Enterprise Solutions for Raytheon's Intelligence and Information Systems business
- Brian Wells, senior principal engineering fellow and chief systems engineer within the Raytheon Corporate Engineering organization
- Marvin Ebbert, special projects member of MS Engineering vice president's staff
- Michael Liggett, director of Technology Programs for Raytheon Corporate Business Development

Warfighter Panel

The MSI symposium hosted an interactive discussion with a six-member warfighter panel. All of the panelists were current Raytheon employees, some of them retired from their military careers and some still serving in the armed forces. They answered questions and provided insightful discussion on topics such as neutralizing our enemies' ability to primitively, but effectively, adapt to our technologies and the creation of a "green bomb."

There were more than 455 attendees, 116 presentations, 10 tutorials and 20 "Birds of a Feather" meetings at the symposium. The MSI Chairs — Paul Benton, Mike Biss and Paul Weeks — and the entire symposium planning team provided a forum for broad collaboration and for sharing MSI capabilities, skills and insights — assisting to establish Raytheon as the premier Mission Systems Integrator and a recognized leader in systems engineering.

Product Data Management:
Changing the Way We Do Business

Imagine a world in which there are common business processes across the company … where a common tool ensures process discipline and predictable execution … where a Web-based work environment enables consistent collaboration … where you are able to retrieve the information you need at your fingertips in near-real time … and where you can design anywhere, build anywhere and support anywhere.

No, this isn't the stuff of science fiction or fantasy. It's the goal of Team Product Data Management (PDM). Team PDM is an enterprisewide team whose mission is to provide a common affordable solution across the company to improve execution and collaboration and drive predictable bottom-line performance.

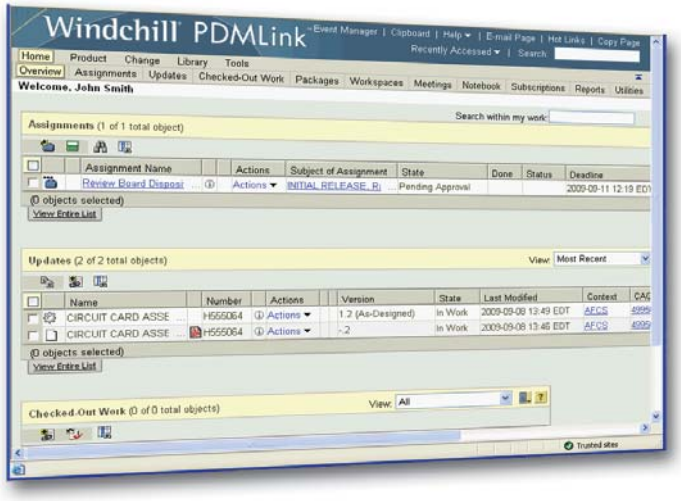
PDM is a business solution composed of common processes and a common tool that will enable us to manage, share and use product data more effectively. PDM will standardize and simplify the design release, product configuration, and technical data package delivery processes through the deployment of Parametric Technology Corporation's (PTC) modern, Web-based Windchill® PDMLink software. PDM will be used across the company to manage product data; ensure predictable execution; and encourage consistent collaboration among Raytheon teammates, suppliers and customers.

Single Tool + Common Processes = A Business Solution

A team of reviewers representing all of Raytheon's businesses selected PTC's Windchill PDMLink software as Raytheon's common PDM tool based upon cost, out-of-the-box tool functionality, supplier performance, usability and risk.

The more difficult part of the equation — developing common business processes — also requires meaningful collaboration among the businesses. Teams of subject matter experts from each business work together to define common processes through a series of workshops. The results include standardized terminology and simplified processes that focus on industry best practices. To date, the processes for initial release, product configuration, technical data package delivery and supplier data requirements list management have been made common across the enterprise.

Additional processes will be standardized as the PDM program moves forward.



Benefits

PDM is going to change the way Raytheon does business by providing more visibility into the design process. Among other benefits, PDM will enable quick searching of product data, including all related documents and drawings, in one tool; easier sharing of information with teammates; and near-real-time knowledge about product-related changes. The result: increased effectiveness and efficiency.

The common PDM solution will enhance Raytheon's ability to be a Customer Focused company based upon performance, relationships and solutions. PDM will help reduce cycle times, increase design reuse and workforce agility, and provide the infrastructure for increased customer collaboration. By enabling Raytheon to design anywhere, build anywhere and support anywhere, PDM will help the company be the most admired defense and aerospace systems supplier through world-class people and technology. ●

PDM Highlights

- A single tool to access product data and drawings
- Ability to search for and retrieve accurate data in near-real time
- Easier design reuse, thanks to greater search capabilities
- Increased visibility into the current status of the design process and knowledge of changes as they occur
- Enhanced collaboration with teammates, business partners and suppliers
- Increased workforce agility and ability to share work between programs
- Fewer training hours and decreased support costs once PDM is deployed across the enterprise

Steve Olive on the PDM Solution

Over the past two years, I have led an enterprise team focused on achieving a vision: Design anywhere, build anywhere and support anywhere. As a former CIO, I felt leading the Business Solutions and Integration team was a natural transition. I soon realized the many challenges of leading an enterprise team — a tiger team that needed to think and act differently. However, the opportunities have surpassed the challenges.

Leading the PDM program has provided me with exposure across the businesses and deepened my understanding of both the business processes and tools. But I believe that without the alignment and engagement of the people, we will not achieve our vision and change the way we do business. Our people are the key to success.

I have talked to employees, partners and suppliers about Raytheon's common Product Data Management (PDM) solution, and I see their enthusiasm as they envision PDM's possibilities. The enterprise PDM team is committed to changing the way we do business at Raytheon. Our vision is becoming a reality, and the energy is contagious.

With PDM, Raytheon's world-class people will be armed with common processes and standard workflows enabling collaboration, ensuring process discipline and opening doors for career mobility. Suppliers will be able to share information more effectively and efficiently, strengthening our ability to partner to create new, affordable solutions. Our customers will benefit from faster, more agile and more precise execution and response.

Through a common PDM solution, Raytheon is building the foundation for its design anywhere, build anywhere and support anywhere vision. Once realized, this vision will truly change the way we do business, positioning us for ongoing growth — and more important — ensuring our customers' continued success in their missions.

Stephen R. Olive
Vice President, IDS Business Solutions and Integration (2008-Jan. 2010)*

**Olive was appointed VP and Deputy for IDS Operations and Supply Chain in Feb. 2010*

IP Track:
Enabling Innovation and Protecting Raytheon's Intellectual Property

At Raytheon, innovation takes place all around us; it's part of our history, drives our future, and can come from anywhere in the organization. As mentioned in "Technology Today," Issue 1, 2009 — "Raytheon's Culture of Innovation" — inclusiveness of innovation is a key method of addressing our customers' needs. To protect Raytheon's legacy of innovation, we obtain patents and trademarks from the United States and foreign patent and trademark bodies. We developed a new tool, called IP Track, to increase the efficiency of filing patent and trademark applications.

Before a patent or trademark application is filed at the U.S. Patent & Trademark Office or a foreign patent or trademark office, the invention or mark is subject to a series of internal reviews, a process that is handled by the Intellectual Property & Licensing Department (IP&L), and the company's intellectual property attorneys.

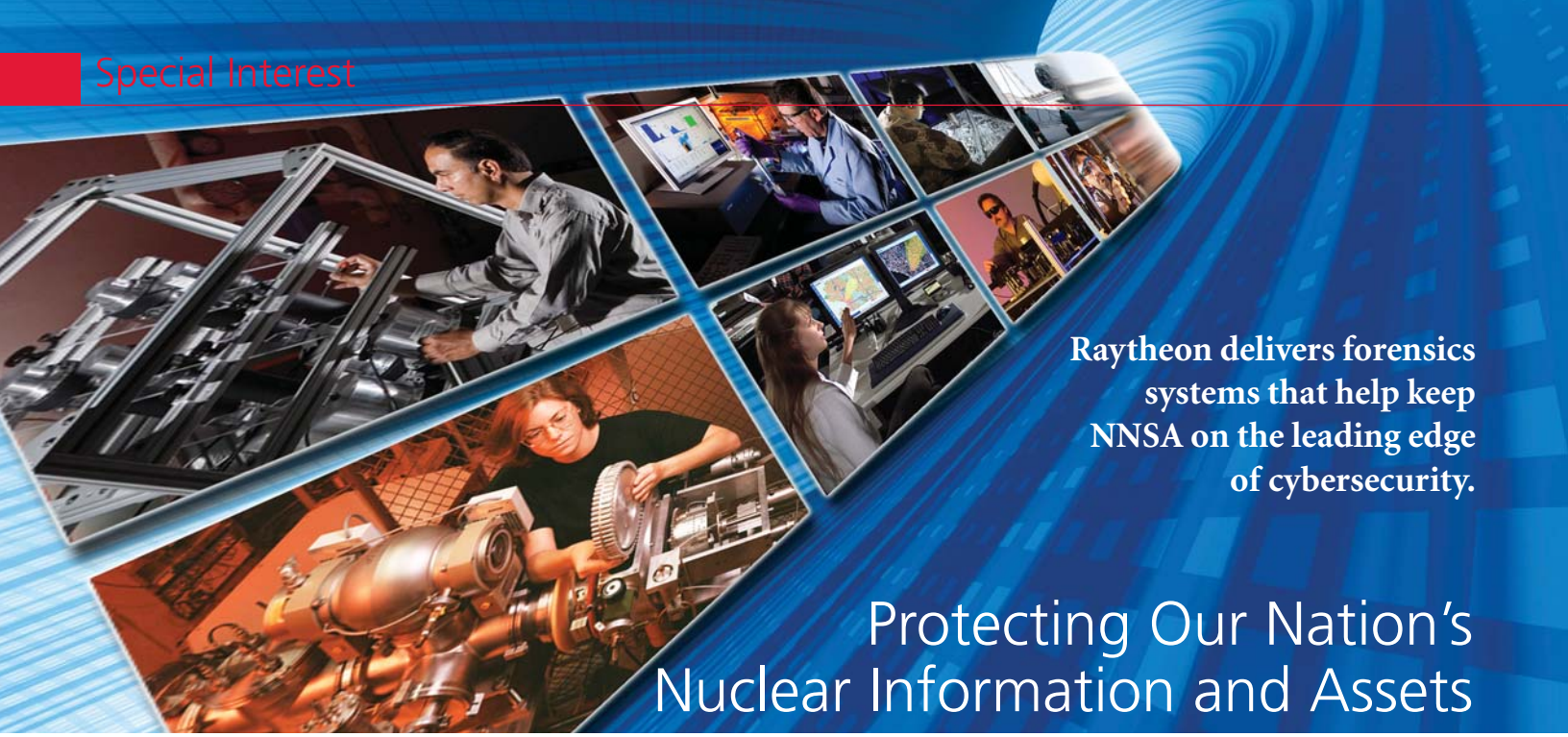
IP&L embarked on the IP Track project with the goal of deploying a new technology that enables efficient entering and tracking of all internal IP processes. Raytheon purchased a leading commercial off-the-shelf software package designed to automate internal IP processes, including patents, trademarks, license agreements and domain names. The IP Track project team completed final data conversion and deployed the tool late last year. The efficiency of the system makes it easier for inventors to submit inventions, leading to increased patent filings for Raytheon.

The software's modular design is flexible, allowing Raytheon to mold the features of the tool to our IP needs. Working closely with supplier consultants, the IP&L team has refined its internal invention disclosure, invention review, and patent and trademark filing processes using IP Track, to simplify and enhance invention and trademark tracking. Relative to patent filings, the solution uses a Web interface to give inventors and technical directors a level of access that they have not previously had. IP Track streamlines the submission process of an invention disclosure with an intuitive Web form that reduces the time required to enter an innovation into the process.

A streamlined system and simplified process encourages inventors to submit their innovations and increase the number of valid inventions filed by Raytheon. The tool continues to show its capability with enhanced tracking features; an inventor or technical director can quickly view all of their submissions with a current status of where the invention stands in the review cycle.

Innovation is challenging, but with IP Track the submission of inventions doesn't have to be. ●

Concetta Veasie
concetta_m_veasie@raytheon.com



Raytheon delivers forensics systems that help keep NNSA on the leading edge of cybersecurity.

Protecting Our Nation's Nuclear Information and Assets

"To enhance national security through the military application of nuclear energy" and "to reduce global danger from weapons of mass destruction (WMD)."Those are just two of the national missions specified by Congress when it established the National Nuclear Security Administration (NNSA) in 2000. Today, NNSA has eight major facilities nationwide, with countless buildings and structures housing some of our country's most intricate and important national security work and information assets. These critical assets range from the world's fastest supercomputers processing sensitive nuclear data that ensure the safety of the nation's nuclear stockpile, to advanced technologies for detecting WMD proliferation. NNSA's information systems must be secured against cyberattack and compromise — protection of these information assets is paramount to our nation's security.

To meet the demands of a dynamic cyberthreat environment, NNSA needed to move from its disparate, site-specific, classified network infrastructure to a secure enterprise solution. As prime contractor and systems integrator, Raytheon worked with NNSA to research, plan, implement, test and accredit the Enterprise Secure Network (ESN). This highly secure network enables NNSA sites and laboratories across the country to better share classified data in a secured enterprise environment.

A Proven Partner for Safeguarding NNSA Systems

For more than nine years, Raytheon has delivered secured, integrated intrusion analysis and computer forensics systems to keep NNSA on the leading edge of cybersecurity. During ESN development and implementation, we provided program and project management, network engineering, system administration and help-desk support — as well as network and security operations facilities management — to prevent and detect threats. Located at the U.S. Department of Energy's Cyber Incident Response Capability, or DOE-CIRC, in Las Vegas, the operations facilities are a Raytheon-developed and managed center for enterprisewide intrusion analysis and cyberforensics services.

Built with commercial off-the-shelf hardware and software and by implementing security best practices, Raytheon's ESN system solution provides enterprise-level access management in a highly complex, classified environment. After extensive integration, testing and certification, the ESN is now deployed to NNSA laboratories and plants, encompassing all communications and computing systems and services, software applications, system data and security services. Using ESN's two-factor, federated authentication based on Security Assurance Markup Language (SAML), general users can access Web-based applications at other NNSA sites. The ESN is among the first uses of SAML for federated, cross-site authentication of users and authorization to resources on one major government network. Enhanced security features include need-to-know restrictions and network monitoring.

Meeting Tomorrow's National Security Needs

The ESN is both critical to the security of the nuclear weapons program and essential to transforming the Cold War nuclear weapons complex into a 21st-century national security enterprise. The network is a crucial component to the NNSA's Complex Transformation — the agency's vision for a smaller, safer, more secure and more cost-effective national security enterprise.

As NNSA continues to evolve, the foundation of Raytheon's ESN solution supports the long-term vision of secure information sharing across a wider set of agencies and boundaries. The next phase of ESN enhancements includes a cross-domain Secret Internet Protocol Router Network, or SIPRNet, Gateway to transmit classified information to the U.S. Department of Defense and other government agencies. The future also holds a similar installation of security mechanisms and infrastructure in the *yellow* or *sensitive but unclassified* environment.

For information contact debra.j.tighe@raytheon.com ●

U.S. Patents
Issued to Raytheon

At Raytheon, we encourage people to work on technological challenges that keep America strong and develop innovative commercial products. Part of that process is identifying and protecting our intellectual property. Once again, the U.S. Patent Office has recognized our engineers and technologists for their contributions in their fields of interest. We compliment our inventors who were awarded patents from May 2009 through November 2009.

RAGHUVEER MALLAVARPU
MATTHEW C TYHACH
COLIN S WHELAN
7528649 Method for designing input circuitry for transistor power amplifier

JOHN BEDINGER
JAMES S MASON
S RAJENDRAN
7528792 Reduced inductance interconnect for enhanced microwave and millimeter-wave systems

MOHAMED K NEZAMI
7529295 Acquiring a frequency and phase offset estimates using frequency domain analysis

STEPHEN C DUTKA
7529291 Methods and structures for rapid code acquisition in spread spectrum communications

DAVID G JENKINS
BYRON B TAYLOR
7530528 Methods and apparatus for guidance systems

JAMES G SHEPARD
KALIN SPARIOSU
7531349 Standoff bioagent-detection apparatus and method using multi-wavelength differential laser-induced fluorescence

THEAGENIS J ABATZOGLOU
LEO H HUI
7532150 Restoration of signal-to-noise and spatial aperture in squint angles range migration algorithm for SAR

LAURA A CHEUNG
MOHINDER S GREWAL
PO-HSIN HSU
7532161 Method and apparatus for wide area augmentation system having I1/I5 bias estimation

IKE Y CHANG
JONATHAN D GORDON
IRWIN L NEWBERG
RICHARD W NICHOLS
CLIFTON QUAN
7532163 Conformal phased array antenna and communication system for helmets and other platforms

JAR J LEE
STAN W LIVINGSTON
7532170 Conformal end-fire arrays on high impedance ground plane

BRYAN J CHEN
7532242 Pipelined amplifier time delay integration

MICHAEL S BIELAS
MATTHEW R DANNER
BRIAN T MACINTOSH
7532863 Broadband wireless ad-hoc modem and network testbed

MICHAEL D HOWARD
ERIC HUANG
7533073 Methods and apparatus for heuristic search to optimize metrics in generating a plan having a series of actions

BILLY D ABLES
JOHN C EHMKE
ROLAND W GOOCH
7535093 Method and apparatus for packaging circuit devices

KEVIN W KIRBY
DAVID S SUMIDA
7535947 Enhanced beam quality from a laser rod using interstitial dopants

CHARLES M DELAIR
CHRISTOPHER P OWAN
7537541 Implicitly timed gear bearings

DAVID D CROUCH
7538735 Active transmit array with multiple parallel receive/transmit paths per element

DAVID G JENKINS
RICHARD C JUERGENS
BYRON B TAYLOR
7540449 Methods and apparatus for non-imaging guidance system

GABOR DEVENYI
7541569 Position sensor utilizing light emissions from a lateral surface of an optical fiber

DAVID J KNAPP
DEAN R MARSHALL
7541994 Refractive compact range

ROY P MCMAHON
7544404 Shape-recovering material suitable for application of an attachment, and its use

ALEXANDER C CHILDS
KENNETH A GERBER
ROBERT P GINN
ANDREAS HAMPP
7544532 Infrared photodiodes and sensor arrays with improved passivation layers and methods of manufacture

IRA R FELDMAN
PAUL A MOOSIE
BRIAN E PATNO
7545287 Enforcement transponder

DAVID B SHU
7545307 Target recognition system and method with unknown target rejection

IKE Y CHANG
IRWIN L NEWBERG
7545322 Antenna transceiver system

JOHN S ANDERSON
CHUNGTE W CHEN
7545562 Common aperture optical system incorporating a light sensor and a light source

DAVID D CROUCH
7545570 System for selectively blocking electromagnetic energy

THOMAS K DOUGHERTY
JOHN J DRAB
KATHLEEN A KEHLE
7545625 Electrode for thin film capacitor devices

DOUGLAS M BEARD
GARY H JOHNSON
RENE D PEREZ
JOHN A THOMAS
7547865 Optical element mount and method thereof for a gun-launched projectile

THOMAS K LO
WILLIAM J SCHMITT
RONALD O WHITE
7548184 Methods and apparatus for processing data from multiple sources

THOMAS E WOOD
7548194 Hostile intention assessment system and method

DAVID H ALTMAN
JOSEPH R ELLSWORTH
MICHAEL E NULL
7548424 Distributed transmit/receive integrated microwave module chip level cooling system

KIRK A MILLER
7550965 Angular position measurement device

SHAWN W MILLER
7552037 Simulating a sensing system

LACY G COOK
7556389 Pointable optical system with coude optics having a short on-gimbal path length

STEVEN D BERNSTEIN
WILLIAM E HOKE
RALPH KORENSTEIN
JEFFREY R LAROCHE
7557378 Boron aluminum boron nitride diamond heterostructure transistors

KEITH M BROCK
7557476 Hollow core electric motor

KAICHIANG CHANG
SHARON A ELSWORTH
MARVIN I FREDBERG
PETER H SHEAHAN
7560400 Radome with polyester-polyarylate fibers and a method of making same

DUNG T NGUYEN
7562501 Clamping apparatus

JOHN A COGLIANDRO
JOHN M MOSES
7562708 Method and apparatus for capture and sequester of carbon dioxide and extraction of energy from large land masses during and after extraction of hydrocarbon fuels or contaminants using energy and critical fluids

DOMINIC S NUCCITELLI
7562908 Flexible fluid conduit joint and method

ERIC L HANSEN
7564347 Dynamically tasking one or more surveillance resources

GARY A FRAZIER
ROGER K LAKE
7564390 Optical digital to analog converter

GERALD C CHIANG
FRANK C LAM
7566026 Onboard guidance method for ballistic missiles

GARY H JOHNSON
7566028 Integral locking mechanism for deployable device

REZA M DIZAJI
HAMID GHADAKI
7567203 Classification system for radar and sonar applications

CHUL J LEE
7567205 Dynamic ray traversing

FRANK A BIRDSONG JR
JOSEPH J FRAUNDORFER
DARRELL L YOUNG
7567627 Estimating the location of a transmitter according to phase differences

MATTHEW FASSETT
JAMES C MCRAE
DANIEL T MCGRATH
KUANG-YUH WU
7576701 Rotating screen dual reflector antenna

GABOR DEVENYI
7578211 Leadscrew drive with annular-shell leadscrew

QUENTEN E DUDEN
7578482 Catalyzed decomposing structural payload foam

JOHN F BUGGE
CHARLES M DELAIR
ERIC M LAFONTAINE
JERRY D ROBICHAUX
7579799 System and method for determining angular position and controlling rotor orientation

JOHN A COGLIANDRO
PIALI DE
AMIR W HABBOOSH
JOHN E RANNENBERG
JOE R WANG
7580818 Mission profiling

PIALI DE
JOHN E RANNENBERG
7580819 Adaptive mission profiling

STEVEN A COTTON
BENJAMIN P DOLGIN
BRETT GOLDSTEIN
DONALD K GRINDSTAFF
JOHN L HILL III
MICHAEL SHELKIN
JORAM SHENHAR
WILLIAM G SULIGA
DAVID C VICKERMAN
JOHN G WITZEL
7584808 Centralizer-based survey and navigation device and method

CHRISTOPHER L FLETCHER
DAVID J GULBRANSEN
7586074 Multi-mode high capacity dual integration direct injection detector input circuit

MARY D ONEILL
GREGORY K PIERCE
WILLIAM H WELLMAN
7586075 Method for analyzing output data of array sub-elements of an imaging segmented array

ALEXANDER A BETIN
NATHAN P DAVIS
JOSEPH J ICHKHAN
7589890 Conductively cooled liquid thermal nonlinearity cell for phase conjugation and method

LACY G COOK
JOSHUA J THORNES
7589896 Optical pulse-width modifier structure

GARY A FRAZIER
7590401 Super-regenerative microwave detector

LACY G COOK
ERIC M MOSKUN
HOWARD M DE RUYTER
7592588 Calibration source infrared assembly for an infrared detector

KENNETH A GERBER
ROBERT P GINN
7592594 Method of construction of CTE matching structure with wafer processing and resulting structure

CHUL J LEE
7592947 Generating radar signatures for multiple objects

CHETAN GANDHI
REINHARDT W KRUEGER
STAN W LIVINGSTON
7595688 High power commutating multiple output amplifier system

JAR J LEE
STAN W LIVINGSTON
CLIFTON QUAN
7595760 Airship mounted array

MICHAEL A MOORE
JAMES S WILSON
7595988 Thermal management system and method for electronic assemblies

PHILLIP I ROSENGARD
7596560 System and method for adaptive query identification and acceleration

THOMAS DOYLE
DIANA P SCHAEFFER
7597047 Simulating an explosion of an improvised explosive device

SAMUEL J RODRIGUEZ
7597527 System and method for transporting an object in multiple directions

ANTHONY O LEE
CHRISTOPHER A ROTH
PHILIP C THERIAULT
7599138 Adjustable optical mounting

RONALD T AZUMA
MICHAEL J DAILY
JON N LEONARD
HOWARD E NEELY
7599789 Beacon-augmented pose estimation

JOE H LINDLEY
7599819 Method and system for generating a predictive analysis of the performance of peer reviews

EMERALD J ADAIR
JUDITH K CLARK
GRAY E FOWLER
MICHAEL M LIGGETT
7601287 Method and apparatus for preform consistency

BRIAN J HARKINS
CHUL J LEE
ANDREW P SIMMONS
7602332 Reducing scattering center data using multi-volume aggregation

RICHARD P DONOVAN
STEPHEN P LEBLANC
JOSEPH S PLEVA
7603097 Vehicle radar sensor assembly

POLWIN C CHAN
TIMOTHY E DEARDEN
MARK S HAUHE
CLIFTON QUAN
STEPHEN E SOX
SAMUEL D TONOMURA
TSE E WONG
7605477 Stacked integrated circuit assembly

JAR J LEE
STAN W LIVINGSTON
CLIFTON QUAN
7605767 Space-fed array operable in a reflective mode and in a feed-through mode

RICHARD M WEBER
7607475 Method and apparatus for cooling with coolant at a subambient pressure

TERRY M SANDERSON
7608985 Method of detecting acceleration in vehicles

JAMES G SMALL
7609001 Optical magnetron for high efficiency production of optical radiation and related methods of use

JOHN C TREMBLAY
COLIN S WHELAN
7609115 Method for designing input circuitry for transistor power amplifier

RUSSELL H ATEN
BRIAN J DANLEY
TIMOTHY I HARDING
SIMON J HENNIN
ANTHONY J JAGODNIK JR
STANLEY J POWERS
ROBERT J STAMM
7616149 Method and apparatus for radar time sensor

JOEL E LAMENDOLA
AARON T SPETTEL
7612710 Processing virtual and live tracks to form a virtual-over-live environment

LEWIS PETERSON
7612731 Methods and apparatus for reducing radio frequency interference for collocated antennas

VETIS B DAVIS
JOSE I RODRIGUEZ
7614175 Method and apparatus for rapid mounting and dismounting of a firearm accessory

BRIAN J HARKINS
CHUL J LEE
7616151 Reducing scattering center data using magnitude-based reduction

DANIEL R CORMIER
TRACY V CRAMER
SUNG I PARK
7616565 Network communication scheduling

ERIC G ROLFE
7619555 Methods and apparatus to contact aircraft

DEANNA K HARDEN
SHERIE M JOHNSON
THOMAS E STAYONOFF
GREG S WOLFF
7620537 Distributed communications effects module

RICHARD M LLOYD
7621222 Kinetic energy rod warhead with lower deployment angles

KENNETH W BROWN
7623088 Multiple frequency reflects array

International
Patents Issued to Raytheon

Titles are those on the U.S.-filed patents; actual titles on foreign counterparts are sometimes modified and not recorded. While we strive to list current international patents, many foreign patents issue much later than corresponding U.S. patents and may not yet be reflected.

AUSTRALIA
ROBERT F ANTONELLI
DAVID W HARPER
DENNIS M PAPE
WAYNE L REED
RICHARD W SEEMAN
2004264438 Loading system for securing cargo in the bed of a vehicle

DAVID L STEINBAUER
2005332959 Reducing antenna boresight error

RANDY C BARNHART
JEFFREY B CHREIBER
MELINDA C MILANI
DONALD V SCHNAIDT
2005234486 Data monitoring and recovery

EDWARD N KITCHEN
DARIN S WILLIAMS
2005328648 FLIR-to-missile boresight correlation and non-uniformity compensation of the missile seeker

KAPRIEL V KRIKORIAN
ROBERT A ROSEN
2006255681 Technique for compensation of transmit leakage in radar receiver

BELGIUM, GERMANY, GREAT BRITAIN
JOHN R STALEY
1723383 Device with multiple sights for respective different munitions

BELGIUM, DENMARK, FRANCE, GERMANY, GREAT BRITAIN, GREECE, ITALY, NETHERLANDS, SWITZERLAND
MARY D ONEILL
WILLIAM H WELLMAN
1308029 Multicolor staring missile sensor system

CANADA
DONALD B HARRIS
JOHN L HILL III
JORAM SHENHAR
2406505 Brake system and method

ROY P MCMAHON
2469621 Shape-recovering material suitable for application of an attachment, and its use

WILLIAM D AUTERY
JAMES J HUDGENS
JOHN M TROMBETTA
GREGORY S TYBER
2419987 Method of making chalcogenide glass

KAPRIEL V KRIKORIAN
ROBERT A ROSEN
2475576 All weather precision guidance of distributed projectiles

ALBERT E COSAND
2458426 Circuit for canceling thermal hysteresis in a current switch

ALDON L BREGANTE
RAO S RAVURI
WILLIAM H WELLMAN
2513017 Sensor system and method for sensing in an elevated-temperature environment, with protection against external heating

ROBERT C EARL
JOHN R GUARINO
ROBERT M OLSON
2569370 Corrosion resistant connection system

JOHN C COCHRAN
JAMES W FLOOR
JOHN HANLEY
WILLIAM M POZZO
2368235 Systems and methods for passive pressure-compensation for acoustic transducers

KAICHIANG CHANG
SHARON A ELSWORTH
MARVIN I FREDBERG
PETER H SHEAHAN
2531848 Radome with polyester-polyarylate fibers and a method of making same

CHINA
QUENTEN E DUDEN
ALLAN T MENSE
2005800359 Catalyzed decomposing foam for encapsulating space-based kinetic objects

DENMARK, FRANCE, GERMANY, GREAT BRITAIN, NETHERLANDS
RICHARD DRYER
GARY H JOHNSON
JAMES L MOORE
WILLIAM S PETERSON
CONLEE O QUORTRUP
RAJESH H SHAH
1377792 Precision guided extended range artillery projectile tactical base

FRANCE, GERMANY, GREAT BRITAIN
PETER V MESSINA
1527319 System and method for automatically calibrating an alignment reference source

RUDOLPH E RADAU JR
PHILIP C THERIAULT
1779170 Imaging optical system including a telescope and an uncooled warm-stop structure

DAVID A CORDER
JEFFREY H KOESSLER
GEORGE R WEBB
1799545 Air-launchable aircraft and method of use

LACY G COOK
LARRY L CUNNINGHAM
RAY D KROLL
ROY A PATIENCE
1483555 Ambient-to-cold focus and alignment of cryogenic space sensors using uncooled auxilary detectors

RONALD R BURNS
MICHAEL J DAILY
MICHAEL D HOWARD
CRAIG A LEE
1393540 Teleconferencing system

KATHERINE J HERRICK
1790033 Reflect antenna

MICHAEL G ADLERSTEIN
VALERY S KAPER
1955439 Phased array radar systems and subassemblies thereof

KEN J CICCARELLI
CARL S KIRKCONNELL
KENNETH D PRICE
1503154 Stirling/pulse tube hybrid cryocooler with gas flow stunt

JOHN E ALBUS
GRACE Y CHEN
JULIE R SCHACHT
1525491 Correlation tracker breaklock detection

FRANCE, GERMANY, GREAT BRITAIN, ITALY
JEFF G CAPARA
LAWRENCE D SOBEL
1425798 Microelectronic system with integral cyrocooler, and its fabrication and use

FRANCE, GREAT BRITAIN, SWEDEN
JOE C CHEN
ALBERT EZEKIEL
1515160 Target shadow detector for synthetic aperture radar

GERMANY
JOHN J DRAB
THOMAS K DOUGHERTY
KATHLEEN A KEHLE
1504460 Improved electrode for thin film capacitor devices

GERMANY, GREAT BRITAIN
CHRISTINA L ADAIR
TIM B BONBRAKE
CHRISTOPHER J RUTZ
1840497 Weapon arming system and method

ISRAEL
PYONG K PARK
160041 Electromagnetic coupling

MICHAEL B MCFARLAND
ARTHUR J SCHNEIDER
WAYNE V SPATE
169080 Missile system with multiple submunitions

JAPAN
JOSEPH M BRACELAND
JEFFREY W DIEHL
MARY L GLAZE
4305595 Mobile biometric identification system

STEPHEN M SHOCKEY
4308666 Method and apparatus for configuring an aperture edge

MITCHELL D GAMBLE
MICHAEL R WHALEN
4326946 Scanning sensor system with multiple rotating telescope subassemblies

NORMAN A LUQUE
4327876 Apparatus and methods for split-feed coupled-ring resonator-pair elliptic-function filters

DOUGLAS M KAVNER
4334870 Vehicle trip determination system and method

ROBERT F ANTONELLI
DAVID W HARPER
DENNIS M PAPE
WAYNE L REED
RICHARD W SEEMAN
4339355 Loading system for securing cargo in the bed of a vehicle

YUEH-CHI CHANG
MARIO DAMICO
BRIAN D LAMONT
ANGELO M PUZELLA
THOMAS C SMITH
NORVAL L WARDLE
4339384 Extendable spar buoy for sea-based communication system

STEPHEN C JACOBSEN
4342318 Resonant electrical generation system

JIM L HAWS
BYRON E SHORT JR
4357780 Method and apparatus for cooling with a phase change material and heat pipes

JOSEPH A ROBSON
GARY SALVAIL
CHAD M WANGSVICK
4358885 Compact broadband antenna

TIMOTHY R HOLZHEIMER
4362677 Circular direction finding antenna

BRUCE R BABIN
4363981 Externally accessible thermal ground plane for tactical missiles

RICHARD M LLOYD
4372755 Fixed deployed net for hit-to-kill vehicle

PERRY MACDONALD
4376940 Low-profile circulator

MALAYSIA
CARL E MCGAHA
BU6351 Method and system for electrical length matching (electrical length matching for cat-5 twisted pair wire)

NORWAY
DAVID A FAULKNER
RALPH H KLESTADT
ARTHUR J SCHNEIDER
1327414 Precision-guided hypersonic projectile weapon system

RANDY C BARNHART
JEFFREY B CHREIBER
MELINDA C MILANI
DONALD V SCHNAIDT
1859546 Data handling in a distributed communication network

PHILIPPINES
JAY P CHARTERS
GERALD L EHLERS
2004500946 Semiconductor article harmonic indentification

RUSSIA
QUENTEN E DUDEN
2359879 Catalyzed decomposing structural payload foam

MICHAEL A BRENNAN
BENJAMIN P DOLGIN
LUIS B GIRALDO
JOHN L HILL III
DAVID K KOCH
MARK LOMBARDO
JORAM SHENHAR
2362879 Drilling apparatus, method, and system

SINGAPORE
PHILLIP A COX
JAMES FLORENCE
127644 Electronic sight for firearm, and method of operating same

SHANNON V DAVIDSON
126454 On-demand instantiation in a high performance computer (HPC) system

TAIWAN
QUENTEN E DUDEN
I-313969 Catalyzed decomposing structural payload foam

Raytheon's Intellectual Property is valuable. If you become aware of any entity that may be using any of Raytheon's proprietary inventions, patents, trademarks, software, data or designs, or would like to license any of the foregoing, please contact your Raytheon IP counsel: David Rikkers (IDS), John J. Snyder (IIS), John Horn (MS), Robin R. Loporchio (NCS and Corporate), Charles Thomasian (SAS), Horace St. Julian (RTSC and NCS).

Raytheon

Customer Success Is Our Mission