Professional Notes

Print [1]

-  [2]
-  [3]
-  [4]

Proceedings Magazine - March 2015 Vol. 141/3/1,345 [5]

"The Next Generation" of Afloat Networking

By Lieutenant Travis Howard, U.S. Navy

The future of the shipboard information-technology (IT) infrastructure was hinted at in *Star Trek: The Next Generation* . Many episodes referenced or discussed the "ship's computer," or the "computer core," as the centralized processing center for the entire ship. Computer functions could be accessed from anywhere on board, even bulkhead panels in the passageways. The fictitious starship had multiple cores that could share the load—or take it on entirely in the event of a failure. These concepts, created by science-fiction writers in the 1980s and '90s, are now real systems that companies such as Hewlett-Packard have built for their clients. [1] Even the *Star Trek* concept of natural language interface—allowing a character to address the computer, which responds to voice commands and can even control the ship's systems without touching a console—is being actively developed by Google as the future of computer and Internet-search algorithms. [2]

Then-Department of the Navy Chief Information Officer Terry Halvorsen recently released a memorandum describing the strategic objectives of information management through Fiscal Year 2018. The theme was clear: We must cut costs to meet fiscal realities. The memo outlined an ambitious plan that doesn't seem to mesh with the slow-moving network management we have created afloat and ashore. Virtualization of the vast majority of IT infrastructure was proposed, as well as the conversion of "90 percent of applicable Navy-Marine Corps Intranet/Next Generation Enterprise Network users to zero-client computing." [3]

This is a radical shift from the "fat" (fully-functional personal computers [PCs]) client-server architecture, a construct that has been the staple of Navy networks for almost two decades, but this strategy change has been a long time coming. Client-server architecture is expensive, wasteful of computer resources, and has proven unsustainable when one considers life-cycle maintenance across 250-plus ships (not counting Military Sealift Command and other commands with deployable networks). A thesis study at the Naval Postgraduate School in

2011 by Lieutenant Jeremy Britt concluded the total cost of ownership of "fat" client-server networks to be much larger than "thin" (stateless desktop terminals dependent on the master server) client architecture, even with added migration costs. Furthermore, thin clients draw less power than full PCs, reducing the combined electrical load of the network. [4]

The Consolidated Afloat Network and Enterprise Services (CANES) program condenses, combines, refines, and delivers on some cloud concepts such as virtualized servers and thin clients for coalition networking services, but even this program is proving too costly ($435 million in FY 13, average unit cost of about $10.9 million) and time-consuming to be sustainable, with a deployment plan to field CANES to just "190 ships, submarines and maritime-operations centers by 2021." [5] CANES still has the same problems as previous network architectures with regard to cyber-security vulnerabilities and the manpower required to maintain this network on each ship.

To reduce total operating costs, save on manpower, and increase our security posture all at the same time, we must design our ships' IT infrastructure the way Gene Roddenberry designed his fictional starships: by moving to a total zero-client, virtualized network environment afloat.

Implementing the Cloud

Major disadvantages of cloud-based, zero- or thin-client architecture must first be considered, but they can be mitigated with proper planning and implementation. The single point of failure resides at the server. If it goes offline, the attached clients will as well. Current afloat architecture operates in a similar fashion for most critical shipboard applications and data (i.e., losing the domain servers means losing email, web browsing, share drive, etc.), so not much would change. However, proper usage of uninterruptable power supplies, data backups, and redundant array of independent disks configuration can mitigate the chances for failure. Additionally, the technology exists to create mirrored redundancy in critical networks such as a ship's classified systems, which allows for a secondary server to restore critical functionality such as command-and-control or intelligence-gathering systems in the event of damage to the primary-server rack(s).

This type of architecture requires low-latency, reliable network connectivity throughout the internal network architecture. Gigabit Ethernet has already been fielded to many Fleet units. Coupled with fiber-optic cabling, it provides stable connectivity with enough bandwidth for virtualized zero- or thin-client architecture. This describes how the thin client network will perform "inside the lifelines" as more capable, high-bandwidth, wideband communication satellites become available. With more terminals such as the Navy Multiband Terminal to take advantage of these satellites, cloud-based services to the warfighter could become available and more easily integrated with the existing shipboard network—without the need to impact the client workstations, as nearly all upgrades would happen at the servers.

The Navy would surely incur significant short-term costs to shift to this architecture, but it would benefit from the concept of accumulated production, the experience gained and cost savings from producing a product over a period of time. As Britt concluded in his NPS thesis, "Migration costs are more than offset by the overall savings and increased life cycle of the thin client." [7] This is further mitigated by existing CANES architecture, as the AN/USQ-208(V) system boasts many of the foundations for a private cloud-based, zero or thin client design. Shifting a shipboard network from legacy Integrated Shipboard Network System to a CANES-based thin-client design would be costly, but upgrading from CANES to a thin-client design is a logical design stepping-stone, and much of the existing CANES architecture could be used.

The loss of cloud capability in an anti-access/area-denial environment is another potential disadvantage. Shipboard networks must operate the "private cloud" by retaining all mission-essential functions within the lifelines via its on board servers. NPS students, such as Lieutenant Stefan Gillette, who envision a "multi-ship afloat cloud infrastructure" have experimented with this "tiered" cloud architecture with great success. [6] Additional research and design efforts must move forward to find the right balance of private (in-hull) and off-hull cloud support, for both administrative services and command-and-control (C2) networked systems that provide a group commander with a common operational picture.

Thin-Client Advantages

There would be many positive results from implementing zero- or thin-client architecture. For example, there would be a long-term cost reduction, since zero clients have a long lifespan; therefore, there would be fewer PC tech refreshes. Zero clients can be ruggedized to offer more endurance than regular PCs and they can run drops to main/auxiliary spaces not previously advised for full PCs. Switching to a thin-client architecture could create the

possibility of one day expanding the network to mobile devices that could be connected to the same services as permanently-installed workstations through virtualization.

There would be fewer security vulnerabilities and information leaks, as information assurance and computer network-defense efforts would be focused to a few critical devices instead of patching hundreds of PC-based workstations. The insider threat would be mitigated by controlling user access to server-side files and data exfiltration methods directly from the server. Multiple IT-monitoring functions could be consolidated through virtualization, and decision-supporting systems such as dashboards and roll-up reporting could make network management a more fluid and logical process rather than a complicated technical problem.

Because thin or zero clients require fewer repairs, clients could simply be replaced, reducing the amount of hours spent troubleshooting. Ships could carry several replacement clients; their small form factor and negligible weight would make storage of these replacement clients easier for ships with limited space.

The Navy would be able to expand its private cloud architecture to a hybrid cloud in the future by connecting non-mission-essential administrative processes through off-ship connectivity. A tiered approach to cloud computing could offer increased capabilities, such as a carrier strike group or amphibious ready group tactical cloud that connects through the flagship (an evolution on today's Collaboration at Sea), and an enterprise-wide or DOD-level cloud that connects to the greater DOD information network for administrative functionality and application data replication. [7] The Naval Tactical Cloud concept, described as the Navy's "future multi-intelligence cloud-based collection and dissemination framework," would become a critical player in the hybrid cloud architecture. [8]

A server-thin-client architecture draws less power than its "fat" client-server counterpart. Britt's NPS thesis referenced a commissioned power consumption study by the Wyse Technology Corporation, which found that a fat client-server architecture with 1,000 computers drew approximately 170,000 watts, while a similarly-sized network of a thin-client design drew 92,000 watts. [9]

The Future Afloat Strategy

One of the primary tenants of the Information Dominance Corps' strategy for the future is assured command and control (C2). The Navy's *Strategy for Achieving Information Dominance* , penned by the Deputy Chief of Naval Operations for Information Dominance in 2013, pointed out that "sensing the environment, understanding our adversaries, and operating and defending our communications and networked systems are inextricably linked to the assurance of C2." [10] Work has already started at institutions such as NPS to find ways to field cloud-based solutions to mobile military units, and a 2012 NPS thesis demonstrated that such an architecture was possible and discussed many proven advantages. [11] This research must accelerate and become a focused effort across even more of academia and the Space and Naval Warfare Center, along with authoritative cost and manpower studies for decision makers on how and when to employ this new architecture, particularly with new warship construction as well as upgrading existing systems.

Given the level of expertise, training, and manning in the Fleet now and for the foreseeable future, developing a defendable network architecture is paramount. The next generation of the afloat network—employing zero-client/private-cloud architecture with a robust central-security suite—is a very realistic solution to assuring the network readiness and C2 of our forces. This consolidates the security and administration picture into something manageable by a small crew while still providing the survivable network services that the warfighter needs.

CANES will lay the groundwork for such a future shipboard network by reducing the burden of maintaining legacy systems with critical security vulnerabilities. This is the only way the Navy will fully realize the benefits of CANES —a common shipboard architecture and standardized training pipeline. However, CANES is not the final answer, as described by Rear Admiral Christian Becker, program executive officer of Command, Control, Communications, Computers, and Intelligence, and the flag officer overseeing the implementation of CANES. "As we install CANES we create a platform where we can evolve our capabilities," he said. [12]

The fielding of CANES must accelerate to replace the critically vulnerable and manpower-intensive current afloat network architecture. The Navy should continue the discussion of thin-client cloud architecture and push its advantages to the afloat users. Our warfighters at sea deserve nothing less than the very best, most secure, and most efficient system that we can field. Operating forward with combat-ready forces is our core business, and the networks we rely on daily must be ready to operate efficiently and safely in an evolving cyber-threat environment. The technology, network engineering, and design capabilities exist now for an afloat networking environment that "boldly goes" where no Navy has gone before, and would deliver unprecedented C2 capability to the warfighter.

1. Hewlett Packard, “Why Thin Clients,” 11 November 2013, www8.hp.com/us/en/campaigns/thin-client-solutions/why-thin-clients.html.

2. Eric Mack, “‘Star Trek’ computer inspires future of Google search,” *CNET News* , 13 March 2013, http://news.cnet.com/8301-17938_105-57574187-1/star-trek-computer-inspir... [6] .

3. Department of the Navy, Chief Information Officer, IM/IT/Cyberspace Strategic Objectives for Fiscal Years 2014–2018.

4. Jeremy L. Britt, “Web Applications and Thin Clients in the Navy,” 2011 thesis, Naval Postgraduate School, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA552270 [7] .

5. Defense Industry Daily staff, “U.S. Navy Leaning on CANES to Integrate Shipboard Networks,” *Defense Industry Daily* , 9 January 2015, www.defenseindustrydaily.com/us-navy-to-lean-on-canes-to-integrate-shipb... [8] .

6. Britt, “Web Applications and Thin Clients in the Navy.”

7. Stefan E. Gillette, “Cloud Computing and Virtual Desktop Infrastructures in Afloat Environments,” Naval Postgraduate School, 2012, www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA562746 [9] .

8. George Leopold, “Navy Looks to Float ‘Tactical Cloud,’” *EnterprisesTech* , Cloud Edition, September 2014, www.enterprisetech.com/2014/09/03/navy-looks-float-tactical-cloud [10] .

9. Britt, “Web Applications and Thin Clients in the Navy.”

10. Department of the Navy, Deputy Chief of Naval Operations for Information Dominance, *Navy Strategy for Achieving Information Dominance, 2013–2017* , www.public.navy.mil/fcc-c10f/Strategies/Navy_Strategy_for_Achieving_Info... [11] .

11. Gillette, “Cloud Computing and Virtual Desktop Infrastructures in Afloat Environments.”

12. Interview with RADM Christian Becker, USN, *C4ISR & Networks* magazine, vol. 13, no. 1 (January/February 2013), 9–15.

Lieutenant Howard is assigned to the staff of Navy Cyber Forces, Suffolk, Virginia, as a cyber-security action officer and training team lead. He is a former surface warfare officer and prior enlisted information systems technician.

The New Paradigm for Cyber Security

By Captain Mark S. O’Hare, U.S. Navy (Retired), and Alfred R. Berkeley III

Traditional “network-centric” cyber defenses intend to prevent a thief from reaching data, while new “data-centric” cyber defenses assume the thief will reach it. The new defenses make information hard to find and impossible to read. The difference between the old and new approaches is profound. By changing the balance of power between predator and prey, it introduces a new price-performance curve for cyber security.

The intelligence community is moving some of its processing to commercially provided “cloud” computing. [1] Part of its rationale was that data-centric cyber security would make the cloud implementations safe. While the media picked up on the outsourcing policy conflict, it failed to address the technologies that make the move safe—it missed the shift from network-centric to data-centric technologies.

“Data-centric” Cyber Security

Conventional wisdom says data-centric security is “encrypted storage.” Too simple, this definition misses the mark. Data-centric cyber security is much more than encrypted storage or encrypted transmission, and it is fundamentally different from what we have all been taught: It is a new paradigm.

At the core of data-centric cyber security, “cryptographic splitting” combines the functions of encryption,

authentication, random bit splitting, communities of interest, fault tolerance, and key management into a single pass-through function. Data is fundamentally transformed into secure, fault-tolerant, and verifiable portions, with reduced key management overhead.

Data-centric cyber security is arriving now for several reasons. First, the failure of traditional methods has focused attention on the need for new methods. Second, entrepreneurs saw the need and invented the new technology. Third and more fundamentally, the computational power required to make data-centric cyber security functional, reliable, convenient, and cost effective has arrived in the form of more powerful microprocessors.

State-of-the-Art Capabilities

These capabilities are the current state-of-the-art for data-centric cyber security:

Encryption , a fundamental capability, is necessary but not sufficient to define the data-centric paradigm. Data-centric cyber security uses any encryption that the user wants to use.

Bit-splitting is the "secret sauce" of the new technology. Technically, it is cryptographic splitting or robust computational secret sharing (RCSS) in a multifactor implementation. RCSS is a relatively new branch on the computer science tree. [2] Bit-splitting takes cipher text and decomposes it bit by bit. It prepares each bit for reassembly and then for physical dispersal. If you have the keys, reassembly is easy; if not, it is overwhelmingly complex.

Physical dispersal places the bits in a user-defined number ("N") of physical locations, or "shares." Information-dispersal algorithms are not new, but using them to distribute randomly selected data at the bit level is. The physical separation can be on a combination of local and remote locations.

Redundancy is provided by adding bits to enable "M" of the "N" shares to rebuild lost or damaged shares. Think of redundant array of inexpensive disks storage. The user can specify what "M" is. ("M" is less than or equal to "N.") The redundancy inherent in cryptographic splitting eliminates the need for copies of copies so prevalent in most data centers today.

High availability is all about "up time" as a percentage of "total time." Having data accessible from multiple dispersed physical locations and requiring less than the total number of shares to restore the data improves the odds of remaining up if one or several locations are unavailable. "M" of "N" provides high availability.

Disaster recovery is the ability to recover from a disaster, man-made or natural. Again, being able to operate from many locations without interruption improves the odds of recovering from a disaster. "M" of "N" provides disaster recovery.

Imperviousness to brute force decryption is a result of the predator not knowing how many shares it needs to recover before starting to break the system. "M" of "N" provides imperviousness to brute force decryption. No complete file exists unless shares are recombined under system control.

Imperviousness to distributed denial of service attacks is a useful byproduct of physically distributed shares and the ability to operate with only "M" of "N" shares available. Locations under attack can be ignored while the business can keep operating out of other physically separated locations.

Authentication is provided to ensure that the data in any share have not been corrupted or tampered. It is about authenticating data, not users. Authentication is performed either on the presplit encrypted data or the individual data shares to detect data corruption due to hardware failure or targeted attacks.

Key management is substantially automated, and most keys are encrypted, split, and dispersed. It's not new, but splitting keys at the bit level and dispersing the bits randomly is. The vast majority of keys are handled inside the dispersed shares. A smaller number of keys are managed externally, providing a simplified multi-tier key management model.

Communities of interest are an important capability. Multi-level security for coalition forces is a typical community-of-interest implementation. While communities of interest are not new, using cryptography instead of physically separate networks to isolate them is. This would prevent the "Snowden effect."

Nuclear controls are mimicked if the system is programmed to require two or more authorized users to initiate actions simultaneously.

Mandatory shares can be implemented, which provide for one or more designated data shares that must be

present for the data to be recombined.

Cloaking is the ability to make the Internet beyond the data-centric software vanish to probing hackers. This is a powerful capability that has won industry prizes.

Rebuilding lost or damaged shares without decrypting the remaining shares is a powerful capability, and it is available in state-of-the-art commercial offerings. Cryptographic splitting provides the ability to rebuild lost or damaged shares without un-encrypting as a byproduct.

File-level security allows single documents to be accessible to specific communities of interest. A single file might be available to one person, or many files to many people, or anything in between.

Divisions of labor can be configured, for example, so that administrators can maintain data but not read it. The cost savings are significant, as are the improvements in security.

Cryptographically separate networks will allow running the Non-Secure Internet Protocol Routing Network, the Secret Internet Protocol Routing Network, and the Joint Worldwide Intelligence Communications Network on a single physical network.

Man-in-the-middle attacks can be thwarted because the network packets can be cryptographically split into shares that can be encrypted with keys that have been established using certificates issued by separate certificate authorities. This creates a "distributed trust model" that provides cryptographic separation within a single communication link. Since bit-split data is cryptographically split and is never whole, a hijacked channel will yield no meaningful or intelligible data to the thief.

Implementing this data-centric paradigm in secure virtual machines can avoid any use of ***shared memory*** . Since that is the playground of choice for cyber mischief, many threats are avoided.

Digital rights management can be enhanced using cryptographic splitting to provide improved file-level security and communities of interest.

The new paradigm meets the relevant requirements of the Federal Information Security Management Act and a series of other hurdles, and can be useful to U.S. government departments and agencies.

'Significant Asymmetries'

The net effect of cryptographic splitting is to keep the data unintelligible when it is at rest (in storage) and in motion (in transmission). Since data are in storage for most of their lives, in transmission for a tiny percentage of their lives, and in process (in the microprocessor) for only a tiny portion of their life cycles, these data-centric approaches to security make the data hard to find and even harder to read if found. Time-wise, this new approach protects most data 99.99999 percent of thier lives.

The technology has a number of Federal Information Processing Standard 140-2, Common Criteria, and Evaluation Assurance Level 4-plus certifications. Because the approach is so radically different, it has been tested quite a bit by people who know what they are doing; the encryption works.

We are looking at a new price-performance curve for cyber security. Like many new technology curves, this one offers better performance at lower all-in costs. It is likely to create unexpected collateral damage to older technologies and their vendors. The described capabilities improve cyber security a lot, but they are not all we need. They help with data at rest and data in motion, but they do not protect data in the microprocessor. Furthermore, while they authenticate data, they do not authenticate users. Strong policy and provisioning will also always be needed in any good security solution.

The new data-centric paradigm creates significant asymmetries between friend and foe. Authenticated friends have the keys, while the foe has an enormous computing load to find and intercept even a single share, thus rendering any intercepted data meaningless.

---

1. Kevin McLaughlin, "Amazon Wins $600 Million CIA Cloud Deal As IBM Withdraws Protest," CRN, 30 October 2013, www.crn.com/news/cloud/240163382/amazon-wins-600-million-cia-cloud-deal-... [12] .

2. Mihir Bellare, Phillip Rogaway, "Robust Computational Secret Sharing and a Unified Account of Classical Secret-Sharing Goals," 14 August 2007, https://eprint.iacr.org/2006/449.pdf [13] .

Captain O'Hare graduated from the U.S. Naval Academy in 1976. He is a former program executive officer of aircraft carriers, and currently the CEO of Security First Corp.

Mr. Berkeley is the former vice chair and acting chair of the President's National Infrastructure Advisory Council. He is also the former president of the NASDAQ stock market and is currently the director of Security First Corp.

Staff Officer Leadership

By Stephen A. Mackey

Congratulations on your new assignment as a staff officer. While headquarters tours are not why most people join the military, they introduce you to people from all areas of your service and force you to develop new analytical and problem-solving skills. They also give you a chance to shape the force you will return to. Here are some of the lessons I learned as I adjusted to my new position as a staff officer at Headquarters Marine Corps after 12 years in a series of operational assignments.

Time and effort was spent developing your leadership skills. While you may not be leading Marines or sailors in this position, you're still a naval service leader.

Don't forget your planning skills. From the time you were an officer candidate, you have learned ways to evaluate the situation, make plans on the way ahead, and convey these ideas to groups of people. Don't discard this tool set just because the people you are leading are not toting rifles or wearing body armor and helmets.

Slow down and adapt to your new setting, but trust your instincts. Service as a staff officer on the macro level is little different than a tactical fight. Staff work has a close fight (action of the day/week), isolating the objective (coordination with those impacted by the staff action), and a shaping fight (resource battles in out years).

Leaders must be technically and tactically proficient. Lighting fires and banging drums will not produce fire support in a combat setting; use of the appropriate technology and processes will. Similarly, sending long and unfocused emails to your leadership will not produce results as a staff officer. Words and knowledge of processes are your tools. You must understand your programs and pass what you know to leaders so they can make informed decisions. More important, you must know how your program connects to others and coordinate products with appropriate parties. Finally, you need to know how to move your items in your organization's staff-action system and how to monitor progress through the "great staff beast."

Keep your staff aware of senior leader interest items and priorities. In some cases, decisions need to be made in minutes or hours. If your people understand your priorities, they will make the right decision in your absence. Keeping your people informed will allow your team to exploit any opportunities that arise.

Refine your processes and products. Before you throw out an existing practice or concept, figure out why it was adopted into the decision-making system. Armed with that knowledge, you can make an informed decision on whether change is merited.

Always have a running unfunded requirements (UFR) list. You may encounter fast-breaking calls from your leadership looking for ways to obligate unforeseen cash. A running UFR list that explains what capacity you can purchase with a cash infusion puts you ahead of the pack as the competition for resources begins. Coordinate with under-executing programs and see if they can give you funds. If so, begin work early to let the money move through the system.

Your moral courage will be tested. If an unfavorable event occurs during your tour, figure out what happened and let your leadership know about it. Failure to disclose means one of two things: Either you lack integrity or are so out of touch with your program that you do not recognize problems. Take the beating up front for the issue. Covering up or waiting too long to report may make the issue worse. Your leaders will help you, but only if they know you have a problem. Give an initial report and provide updates and recommendations as the situation becomes more clear.

Advocate for your program, but not at the expense of those who make greater contributions to the service as a whole. Is an evaluation comment about being sharp in the resource arena worth skewing allocation priorities to the service you came from?

Headquarters tours may lack the excitement and adventure of an operational tour, but they compensate in many ways. A staff tour will allow you to work with a large group of your peers, wake up most Saturdays at home, and will give your body a chance to recover from the wear and tear of your first decade of service. Enjoy your time as this year's new blood.

Mr. Mackey is a retired Marine Corps infantry officer. He served on the Office of the Secretary of Defense Staff, the Joint Staff, the Marine Corps Staff and the staff of two defense agencies. In July 2013 he returned from a tour in Afghanistan as the Senior Adviser to the Afghan Deputy Secretary of Defense.