2014

Evolving Open Enterprise Information Systems (Introducti

Web Content Display

Evolving Open Enterprise Information Systems

Vice Admiral Art Cebrowski introduced the concept of "Information Superiority" as the objective of "Network Centric Warfare" in 1998. Ever since then -- according to myriad watchdog reports and Congressional mandates -- the Defense Enterprise has struggled to match its industrial age acquisition and engineering paradigms with information age requirements.

In 2004, OSD chartered an NPS research initiative to help address this mismatch through a government-industry collaborative approach to evolving Open Enterprise Information Systems. The prime directive of this NPS OEIS research is to heed Einstein's definition of insanity; i.e. to capture approaches to solve the problem that are fundamentally improved over the ones that got us in trouble.

This ongoing NPS research is sponsored today by the Undersecretary of Defense for Intelligence.

Web Content Display

Chris Gunderson is a Research Associate at the Naval Post Graduate School.He is the principal investigator of the Open Enterprise Information System (OEIS) research initiative. This project sponsored by the Undersecretary of Defense for Intelligence and executed in the Northern Virginia. The project objective is to help the government improve its flawed information technology acquisition process through four key activities:

- Establish a collaborative network of government, industry, and academic experts who have succeeded at some aspect of OEIS
- Study Internet successful stories and distill the lessons learned
- Embed lessons learned into familiar government acquisition artifacts
- Work with early adopting pilot projects to verify, validate, refine, and document best practices

Prior to this assignment, Gunderson managed an initiative sponsored by the Office of the Secretary of Defense to create the World Wide Consortium for the Grid (W2COG), a global network of collaborative experts committed to rapidly fielding network centric tools for enhancing global security and peaceful commerce.

Gunderson retired from the US Navy in October 2004 as a Captain following 27 years' service.

His last assignment in the Navy was as Commanding Officer of Fleet Numerical Oceanographic & Meteorological Center, a super computer network operation center in Monterey, Calif.

Prior to command of Fleet Numerical Meteorology and Oceanography Center, Gunderson served as Deputy Oceanographer of the Navy, and helped develop Department of Defense policy for enhancing information system interoperability.

Web Content Display

Let's Stop Stepping on Einstein's Rake!

It's been more than fifteen years since Admiral Cebrowski et al coined the term "Network Centric Warfare" The watershed concept hypothesized that a modern military force could gain

Web Content Display

The Unfortunate Truth of Big Data

The amount of data created globally every day is ridiculously big and increasing exponentially – thanks to Moore's Law. The global ability to store data is a lot less than the ability to create it, but still ridiculously big

Web Content Display

Need-to-Survive (and the Need-to-Shop) Trumps Need-to-Know

Do any of the following questions bother you too?

> "Isn't it just as risky not to share critical information with someone who

"asymmetric advantage" over an adversary through "information superiority." Success required integrating the various individual Defense information systems into a single network of "self synchronizing" nodes.

Ever since then, Defense policy has continually emphasized this requirement for joint information system interoperability. Throughout this period a regular progression of watchdog reports and congressional mandates have documented general failure to achieve the policy objectives despite hundreds of billions of dollars spent. The reports comment that these failures came despite, or perhaps because of, Defense procurement efforts to embrace each new commercial information technology paradigm as it crested the Gartner "Hype Curve."

For the last ten years, and also growing exponentially – again thanks to Moore's Law. The global ability to do something truly insightful with the data, e.g. deliver Valued Information at the Right Time (VIRT), is many orders of magnitude less than ability to generate or store data and is improving linearly at best - Moore's Law has apparently taken a pass on this one. The ability to deliver VIRT is equivalent to what Admiral Cebrowski called "information superiority" in his iconic "Network Centric Warfare" concept.

It seems to me that the most important objective of collecting and processing data is to generate VIRT. In that case, typical "big data" strategies, which after all try to solve the data overload issue by creating more data, are doomed out of the gate. That is, architectures that (a) increase the already huge volume of stored data by tagging it

really needs it, even he isn't 'cleared'?"

"If you don't certify my new, automated, Cross Domain Solution, I'll just use a sneaker net. Isn't a sneaker net is a security violation waiting to happen?"

"New policies say that the 'need-to-share' is just as important as the 'need-to-know.' But…will I go to jail if I don't share?"

"Is the NIPRnet, i.e. the Defense Intranet, really more secure than the open Internet? Isn't NIPRnet a clearly defined hackers' target labeled with a big bulls eye called ".mil." Isn't it safer to

a Naval Postgraduate School research initiative, which has come to be called "Open Enterprise Information System" (OEIS), has tried to help solve the problem. The OEIS approach is to apply a few universal truths, namely:

"You can't solve a problem with the people and processes that created it!"

"You get what you measure, and you get what you pay for!"

"Best way to solve a problem is to ask a bunch of experts who have solved a similar problem before."

"The only effective policies are those based on observing something that already works."

"Effective executives follow three rules: (1) put the right, empowered, people in the right jobs; (2) understand what you are trying to do and how well you are doing; (3) spend all of your resources per #1 and #2!"

extensively with semantic metadata, and (b) replicate the stored data and metadata in multiple locations, only magnifies the find-the-needle-in-the-haystack problem. Indeed, this approach adds more haystacks than finders to the mix.

So, big data strategies should also include information services that are orthogonal to tag and search semantic strategies. I highly recommend Dr. Rick Hayes-Roth's the body of work on VIRT. The EIS Value Assurance Framework (VAF) pragmatically implements Rick's concepts. VAF does that by equating the formal requirement for information system "Interoperability" with ability to deliver VIRT. That is, to be effectively interoperable, the subsystems of an EIS must share data and resources effectively enough to generate actionable information.

> hide out under a ".com" disguise out there amidst the billions of other ".com"s?"

Primitive man invented "security" by guarding the entrance to his cave with a club. Ever since then we've been protecting stuff by locking it behind physical barriers. We consider anything that penetrates the barrier, invited or otherwise, as a threat. Naturally enough, when we got around to thinking about security in context with computers and networks, we applied this same lock down mentality.

Unfortunately, or fortunately, the folks who invented computers and the Internet did not build security into the original design. On the contrary, computer operating systems and routable networks were designed to facilitate sharing irrespective of abstract cyber borders. Therefore, computer

"Truly disruptive innovations sneak in below the radar."

So, the OEIS research initiative has four ongoing activities:

1. Nurture a "dot org" open community of expert practitioners with history of success in some aspect of the OEIS problem space. (There are many aspects! E.g. technology, operations, contracting, Intellectual Property, security, social media, etc…)
2. Study successful distributed, collaborative, information sharing phenomena such as LINUX,

How much is a pound of VIRT worth? VAF quantifies the ability to deliver VIRT by defining (Information Processing Efficiency) as (Valued Bits Processed) ÷ (Total Bits Processed). An information bit is valued, if and only if it leads to better decisions. Decisions are better if and only if they lead to measurably better operational outcomes, i.e. Delivered Information Value. So, VAF describes requirements, risk management strategy, and validation and verification methodologies that contractually compel developers to: a) make the EIS Information Processing Efficiency improve in step with Moore's Law, and b) mathematically couples the exponentially improving Information Processing Efficiency to validated and verified Delivered Information Value. This approach rigorously optimizes the risks and rewards

network security tools and methods tend to be kludgy aftermarket offerings.

Given the kludge, information system Certification and Accreditation (C&A) paradigms tend to be subjective and aligned with the particular concerns of the local C&A authority. Generally C&A documentation defines physical security boundaries, such as the outside of boxes filled with software; identifies threats; matches threats to vulnerabilities; and describes actions taken eliminate or mitigate the vulnerabilities. At some locally agreed threshold level of vulnerability mitigation, the local authority grants the certification and/or accreditation.

Today's set of information system C&A rules and methods were developed decades ago, and are not informed by modern

eBay, eFile, Apps Store, weather service ecosystem, etc., and distill critical success factors. (Why do the few succeed while the many fail?)

3. Co-opt the government bureaucratic artifacts that govern OEIS engineering and acquisition. That is, insert OEIS best practices, effective metrics, and incentives within comfortable boilerplate artifacts. (We call this effort the OEIS Value Assurance Framework (VAF)).
4. Find and assist

associated with cost, performance, and schedule in alignment with COTS IT facts of life. VAF thus assures that the performance of an EIS improves exponentially across its lifecycle.

software engineering logical separation paradigms such as abstract programming languages, service architecture, hypervisors, virtual machines, etc. Further, the people who do the detailed C&A work are not typically software engineers. In my experience these are intelligent, hard working, mission-focused folks doing the best they can with the tools and constraints they must live with. I think we should help them by providing more abstract and adaptive tools and methods appropriate for the world we live in today. Regardless, it is impossible to harvest the efficiencies available from modern cloud, virtual, X-as-a-service capabilities given legacy bottlenecks such as traditional cross-domain transfer guards. After all, these guards enforce physical separation between the otherwise virtual service

likely early adopting projects and enlightened project managers. Refine the VAF as we learn new lessons.

Ten years into the project we've met lots of smart people doing great stuff. We think the lessons we've learned through our work can help a lot of projects. We believe the constrained government budgets can actually help catalyze willingness to move out of comfort zones. That is, we OEIS engineers think that the half empty glass is twice the size it needs to be!

providers.

With that in mind, the OEIS research initiative is working toward identifying a stack of open standards that might define the distributed "security layers" to enable "Network Functional Virtualization" across a "Software Defined Network." Think in terms of metaphorical "weapons grade PayPal." Part of the concept is to make information assurance as verifiable as, e.g., Operational Availability (Ao). That is, we are formulating engineering algorithms and frameworks that will quantify the conceptual "number of nines" associated with any particular logical, distributed, dynamically composed, security-as-a-service architecture. A "need-to-protect" metric like "Availability of Information Assurance" (AIA) with values on a continuum from 0.00000-0.99999 will finally

obviate the need for monolithic assurance measures such as legacy “Protection Levels.” Metrics such as “data perishability,” “data consumer survivability,” “mission urgency 1-2-3-4”, can be baked into logical, assured, “need-to-share-policy-services”.

The requirement for discrete, proprietary appliances called “Cross Domain Solutions” can go away. Instead, Need-to-Protect vs. Need-to-Share decisions can be made and executed, dynamically, case-by-case, across a federated enterprise information system according to pre-established polices, and informed by objective quantification of risk and reward.