

## Developing Security Architectures Using Protected Core Networking Concepts

Highly available networks are designed to ensure that the network is available for transport and communication when it is needed. The North Atlantic Treaty Organization (NATO) is evaluating protected core networking from an architecture standpoint for use in coalition activities. NATO envisions this capability as being the primary means of establishing trusted and highly available communications across the coalition. Each member provides protected core segments, which come together yet operate in a federated framework in relation to each other, and this is illustrated in the figure below. Each segment that is provided will connect via pre-established agreements and operates with three primary guarantees. First is that any communications or transport request receives the highest priority for completion. Second is the assurance that the requested communication will successfully complete, even if individual segments have to automatically reroute the communication. And third is that the security within a segment is specified in the pre-established agreements and is the responsibility of the owner of that segment. It is the user's responsibility to ensure message confidentiality and typically, communications are encrypted by the sender prior to utilizing the protected core so that the content cannot be understood while the message is in transit. The primary function of the protected core is to provide high availability network transport services. The information security and assurance is the responsibility of the users, in terms of content protection.

To give a related example, consider a hive of honeybees. They operate autonomously, yet have a pre-established group purpose that supersedes anything else. There is no central authority telling any of the bees what to do, their roles and associated actions are instinctive. If one or several cannot perform their function, others automatically fill those roles. They were designed for this federated approach. They do not have only a border defense; rather they have a defense in depth plan. And that is in essence how a protected core operates. The mission of the network is paramount. Security, in the classical PCN concept, is left for the segments to administer and enforce inside their specific segments of control. Their only restriction is to ensure they maintain the service level agreement. There is no centralized management control of the segments and no centralized security manager and analysis. What exists is an extreme level of trust between and across segments (coalition partners).

So now that we have said security is not directly part of a protected core, suppose we looked at PCN from another angle. Rather than an implementation approach, what about using the concept of PCN to guide the development of security architecture within an enterprise? Could we do that? And would that enhance the security profile of the enterprise it was protecting? The answer to all questions is "yes" and this paper will present key evidence why that is true. Secure protected core enterprise networks are stronger by design than perimeter based or centralized control security models. Through the examination of key facets of an implementation, we will show why this architectural approach provides stronger security and how it can do that.

The presentation will first review the distinctive characteristics of PCN and show through example, how a PCN operates. We will explore the lack of centralized management and security and detail why these represent good architectural building blocks.

The next part will view the threat landscape with some attention to the advanced persistent threat. We will describe how current methods fail.

The third portion will look at the architectural vision of a secure protected core enterprise model. This allows trust to be built by design, rather than being added on.

Next, we will look at how confidentiality, availability and integrity are enhanced and how such security features as authentication, identity management, endpoint security, and audit/control could be implemented. The salient features of this approach will be discussed, which include: ability to use aggregated authentication within the enterprise, un-flattening the network making it more difficult to map and freely traverse, and federated auditing.

In summary, we will show how PCN architected security is better equipped to handle several types of attacks. We will show an attack timeline in conventional architectures and why the defender response time can be enhanced through PCN architecture. We will also discuss how the attack surface changes from uniform throughout the enterprise to controlled variability and why that makes the attacker's job so much harder to accomplish.

## **The Business Case for a Public-Private Sector Partnership in High Performance Computing**

The famous mathematician Richard Hamming said "the purpose of computing is insight not numbers". For businesses to compete in today's international markets, insight into and understanding of, their markets and products is essential. Massively Parallel Computing(MPC), such as that pioneered in the DOE National Laboratories, is being recognized as a competitive advantage for US industry. The automotive, aircraft, oil & gas and even the financial industries are recognizing that sophisticated, highly complex models of their products and processes do give them a competitive advantage. To build on, and maintain, this advantage the transfer of this exponentially growing know-how in massively parallel computing from the National Laboratories to the private sector is essential. This paper presents examples of where and how MPC is being used in industry and discusses some of the barriers to entry. Also presented is the Hyperion project, which is one solution to the barrier-entry problem, developed by Lawrence Livermore National Laboratory and its private sector partners.

## **New Packaging as a Clutter Reduction Method**

All one has to do is look at a photo of a weapons depot in the Mideast to understand the significant role of packaging as a means of de-cluttering military spaces. A packaging technology has been developed by Bell Labs which is a polyethylene based plastic material with Copper reacted into the polymer chain, referred to as a reactive polymer. This combination allows this recyclable, re-usable plastic to be easily re-sealed in the field with simple tape, allows RF signals to travel through it (allowing for easy RFID tracking of assets) while providing the same or improved barrier and anti-corrosion properties than foils (mil B131 packaging). This reactive polymer technology helps prevent mold and mildew damage, something that Mil B-131 packaging cannot do. Finally, the reactive polymer technology has a substantially lower carbon footprint than the 131 Foil bags. De-clutter has to start with the packaging, and this technology allows it to be done easily.

## **Miniaturized, modular, high resolution X-ray Backscatter imaging as a Blue Force enhancer**

This paper will discuss applications of X-ray Compton Backscatter imaging – a powerful one-sided inspection technology used to examine personnel, vehicles (air, ground and sea based), parcels, and cargo for the presence of potential threats (including suicide bombs, IEDs VBIEDs, explosives, weapons, and other contraband) – in providing a true disruptive influence and a powerful Blue Force enhancer. The presentation will focus on how recent developments, making the technology small, portable, and capable of high resolution output, have expanded the application base beyond its current regime. Use of one-sided Backscatter imaging has already proven effective in uncovering hidden threats in a war zone environment as well as within our country's borders, effectively negating any advantage or stealthiness our enemies might believe they possess. The paper will explain the technology of X-ray Backscatter, and how technology and configuration adaptations have been able to provide a unique advantage to its users. With X-ray Backscatter it is now possible to detect both organic and inorganic threats (i.e. items with both low and high atomic number makeup) hidden in vehicles, containers, and on personnel – all from one side of the object, in a package that provides wide-ranging flexibility. Ongoing government-sponsored programs that build on Backscatter's inherent characteristics will be discussed, and representative imagery will be used to demonstrate its use. In addition, the paper will address complementary techniques, such as forwardscatter that can add additional value.

## **Cyber Warfare-Going on the Offense**

In the world of Cyber Warfare we frequently discuss the firewalls, the anti-virus programs and the many other defensive measures that are utilized to shield our systems from attack. Why is it that this is the only form of warfare that is fought totally from a defensive posture? No one has ever won in combat totally on defense. Shouldn't we consider an offensive capability if we intend to move our major networks to an IP-based architecture?

In the new era of combat where Internet Protocol (IP) enabled sensors and forces interact, distinguishing truth from the volumes of data is a high level task. By linking our systems to the same architecture as internet based systems, we may also introduce the same vulnerabilities as many of those systems. In the Cyber arena it is relatively easy to detect a "denial of service attack". In contrast, false data inserted into the data stream or deceptive targets or other more insidious "data" attacks may go unnoticed. How we determine that we have even been attacked is a serious question. This question is accentuated by the fact that we are now operating routinely with coalition forces that don't always have the same capabilities as our forces. This raises the issue of multilevel security and the sharing of information at a much higher level especially in the war against terrorists. With the frequent reports of civilian casualties, any unvalidated information is basically useless in the fight.

As we extend the range of our weapons outside of the ability of our platform sensors to sense the target, we must rely on off-board assets to supply the targeting information. This requires the real time evaluation of targeting data. This real time functionality requirement is evident in the launching of missiles from UAVs at targets in remote areas of Afghanistan and other areas.

If we are to be able to fight offensively, we must solve the cyber security issues. We must not allow the enemy to control the battlefield. We must be on the offensive in the Cyber war.

## **The Cyclone Engine and its Application to Powering Manned and Unmanned Vehicles or as an Auxiliary Power Unit**

Advent Power Systems' Cyclone engine is a disruptive technology that "Expands Blue Force Capability" and help enable increased power projection in the form of more capable UUVs, torpedoes and swimmer delivery vehicles. Its form factor will enable it serve as an efficient auxiliary power unit for tanks and vehicles and in some cases the prime mover.

The engine's patented technology (TRL-6) provides extremely clean, extremely quiet, reliable power generation. The initial 18 horsepower prototype engine has hundreds of hours of operation. Having won 2008 awards including: Society of Automotive Engineers most innovative product, Green Technology Award, Popular Science Top Ten Innovation of the year, the external combustion engine completely burns any combustible fuel, recycling heat so the engine runs cleaner, cooler and more efficiently than internal combustion engines - virtually zero NOx is created. Scalable from man portable generators to 1MW of output power the engine has a 2.5 to 1 weight to power advantage over diesel and 90% fewer parts. The engine has successfully demonstrated its operation using Moden fuel. It is the only engine able to burn this self-oxidizing fuel. As a result hazardous Otto fuel and Lithium batteries can be replaced with the cyclone engine. Future developments include efficiency testing and the development of 100 and 400 horsepower versions of the engine. For ground vehicle applications the engine is very resistant to small arms fire as there are no oil lines, radiator or associated subsystems required for a gas or diesel engine.

## **Counterspace Capabilities using Small Satellites: Bridging the Gap in Space Situational Awareness**

Advances in miniaturization and proliferation of space technology will provide rogue nations access to very small anti-satellite systems, while geopolitical drivers provide the motivation for countering U.S. sovereignty in space. Small satellites have lowered the cost of entry into the once-elite space club, thus allowing non-traditional countries, such as India, Iran and Taiwan, to become players. This openness to space also creates a new threat from hostile nations. With access to the exact same technological breakthroughs, our nation's satellite communications become exposed to possible unmonitored attacks crippling national security.

No single technology currently envisioned for future timeframes will be able to fully address the need for comprehensive space knowledge. Instead, any potential solution needs to be a system-of-systems that is part of a comprehensive architecture. They must be able to maintain "knowledge custody" of all space objects from the moment of launch, so that if a hostile space attack occurs, the system can produce an "indisputable chain of evidence" leading to attribution. The system must also be able to provide enough information to determine whether a satellite is active and what its capabilities are.

A great deal of work has been done recently with regard to smallsats, also known as microsats, minisats, nanosats, picosats and cubesats. The low cost and rapid insertion into space is changing the face of the way we view satellites. Innovations in manufacturing, miniaturization and fabrication quality have made the concept of smaller, lighter and, thus, lower cost satellites that perform mission critical functions a real possibility. Until recently, their development has remained mostly an academic practice, advanced by universities and small research outfits, but this is changing. With these advancements also comes a dark side. To date, at least 30 countries have operated microsattellites, and China recently established the "world's largest microsattellite industry park."

Consider the following hypothetical scenario. Ten years from today, a Long March 6 rocket lifts off, carrying the Indonesian IndoCom-7C communications satellite. The satellite is placed into geosynchronous orbit to provide wideband communications. The U.S. Space Surveillance Network (SSN) observes the launch, and, within minutes, the Space Based Space Surveillance (SBSS) system computes the IndoCom-7C orbit and verifies that it has been placed into the pre-announced orbital slot. SBSS continues to watch as IndoCom-7C completes its deployment maneuvers and unfurls its solar arrays. After verifying that the IndoCom launch appears nominal, SBSS is re-tasked. Now, six months later, what appears to be a radiator panel on the side of IndoCom-7C swings open. Thirty-two cubes, each about 10 centimeters across, fly out of the IndoCom opening. This event is not detected by the SSN. The cubes automatically configure themselves into an autonomous cluster and silently navigate to their destination. This swarm of miniature satellites, operating as a virtual cluster, approach the MUOS-5 spacecraft. Undetected by any U.S. system, the cluster identifies the main electrical panel onboard MUOS-5 and attacks. Seconds later, MUOS-5 powers off its transponders as the onboard computer malfunctions. Twenty-two thousand miles below, key U.S. Navy ships lose their satellite communication links. This scenario may seem unlikely today, but rapid advances in spacecraft miniaturization, coupled with geopolitical drivers, make such a scenario possible. The future threat, therefore, finds that advances in microminiaturization and proliferation of space technology provide any number of rogue nations access to very small anti-satellite systems, while geopolitical drivers provide the motivation for countering U.S. sovereignty in space.

Lockheed Martin is developing design optimization tools and human expertise to create a comprehensive and accurate modeling and simulation environment for small satellite missions to address these specific areas. We are working on research in two specific areas: (1) enabling technologies and methodologies, advanced concepts and algorithms, and artificial intelligence for protection against small satellites; and (2) advanced research into improving space situational awareness given the threat of adversarial small satellites. Our research will be more fully described in detail at the conference, which includes a series of predictive computer models. For example, for a set of mission objectives, the system will be able to tell the user the best fit (economics and

performance) be it large, small, mini, micro, nano, pico, femto, or a constellation combination. Also, we are further developing DARPA's F6 fractionated concept by taking various subsystem functionalities on conventional satellites and modularizing them on separate smaller satellites that would then function together.

## Super Empowered Individuals

What is disruptive technology? The simple answer is a technology that disrupts. In the military and defense world it means doing something in a manner for which you are not prepared and it disrupts your operations. In Iraq and Afghanistan a disruptive technology has been the Improvised Explosive Device. What made it disruptive was that we were attacked in a way that we had not expected. Our military industrial complex prepared for tanks, close air support, and the grand land battle in Europe. It did not prepare for an IED war. IEDs are not new, they have been around for years. They used to be called booby traps. An IED even started WWI with the assassination of Arch Duke Ferdinand.

Our nation has invested billions in national defense over the last several decades only to be ground to a halt by a device that cost between 50 and 1500 dollars. They employed not from a massive weapons platform like a tank chassis or an airframe but laying on the side of the road. Our answer was to spend 2 billion dollars to develop a newer vehicle with more armor. The enemy countered by using 2 155mm rounds instead of 1. So with very little R&D the enemy cost us billions of dollars in R&D funding. The enemy is super empowered with information at his fingertips, ease of travel, freedom to move and organize and is running rings around our military. What disruptive technology do we have to change that?

The disruptive technology is simple, it is super empowering our military members to fight as super empowered individuals. People are the disruptive technology, and they will never be defeated with machine or technology. We will defeat them by going toe to toe in every environment kinetic and not kinetic. A simple return to the classical lessons of warfare will explain this. War is a violent clash of opposing wills with the intent to impose your will upon the enemy. This requires a paradigm shift away from technology as the means to an end, towards technology as one of many methods.

This requires a re-thinking of our training, a shift away from buttonology towards conceptual understanding. The settlement of the west required several technologies: deep well drilling, repeating arms, barbed wire, and the steel plow. Each on their own were marginal improvement but collectively were disruptive. During the presentation I will discuss how collective disruption is enabled by numerous marginal improvements including but not limited to the operational distributed use of increased computing power, database uses, mashups, GPS, mesh networks, and the potential enemy counteractions across the range of military operation.

## **Real-Time 3D Data Gathering, Visualization, and Data Fusion from Manned/Unmanned Platforms**

With funding from NAVEODTECHDIV, ARDEC, TARDEC, and SPAWAR, Autonomous Solutions has developed and continues to develop a real time 3D world building application that creates fast 3D models and rendering of target locations for use in robotic control tasks, object identification, situational awareness, and remote object measurement. The typical system includes a stereo vision sensor integrated with a GPS/inertial position estimation system and posture encoders, such that a vehicle model can be rendered alongside the world model. To correct for errors in the positioning system, point cloud registration algorithms are used to stitch world models as the user drives the platform through the environment. Thus, 3D worlds can be built and displayed in real time as a user, vehicle, or robot, moves through an environment. These worlds can be viewed from any perspective by multiple users. This data can be geo-registered such that it can be overlaid with existing a priori data to give a constantly updated map. The data can also be stored in a database and used for post-mission forensic analysis and change detection. The stitched models complement large aerial terrain data by providing a higher detail ground based representation of a target. The repository of 3D data can also be accessed for machine automation systems for planning and perception tasks such as recognizing objects, such as doors and stairs, and creating traversable paths through them. This system is also scalable for use with a team of robots, such that collaboration could more efficiently create decentralized 3D databases of a large target area.

## **Carbon Nanotube (CNT) Composites using Solution Spun Fibers**

Carbon nanotube (CNT) composites are being explored for use as robust, low-observable electronic devices in a variety of common articles such as cloth, paper, and plastic, due to their inherent covertness, high conductivity, light weight, high corrosion resistance, and potential to be incorporated into thin films and fibers. This work focused on producing macroscopic fibers from single wall carbon nanotubes (SWNTs) by solution spinning. Multi-filament threads of these fibers had sufficient strength to embroider into cotton and cotton/nylon blends. The SWNT composite materials are transparent to X-ray scanners, and, in some cases, optically transparent. The electrical properties of composites prepared from SWNT threads were evaluated. The results suggest that lower losses may be available from thread-based structures than from thin-film devices.

## **Open Architecture (OA) is Business Change**

This paper describes why the business imperatives of Open Architecture (OA) are much more important than just a technology enhancement. In fact, focusing on the technology is a potential risk technique used by the incumbents to dilute the criticality of introducing competition as the means of delivering timely, cost-effective combat capability. Doing OA is the opportunity to accelerate new business methods supporting emergent warrior's needs, while reinvigorating engineering talent and recruitment across the Defense infrastructure. Finally, an effort is made to describe how the current U.S. Navy surface battle management systems could innovatively transform for a more adaptable, sustainable, and thereby more competitive operationally in an uncertain world.

## **Cyber Tradecraft & OPSEC: Techniques and Technologies to Retake the Internet High Ground**

**PROPOSED CONFERENCE CATEGORY:** CYBER DEFENSE, OPERATIONS AND ATTACK

**Type:** Oral presentation with accompanying PowerPoint

Despite the fact that the Internet was invented in the United States, the U.S. government has effectively abandoned it, choosing instead to retreat to a private enclave behind its walls. The virtual world has become an enemy held territory and is now a primary training, recruiting, and fundraising mechanism for U.S. enemies who routinely use cyberspace as a valuable tool to plan operations and rally networks around the globe.

Government agencies who investigate nefarious online networks in search of credible intelligence encounter real and present dangers every time they conduct online missions. The importance of understanding the risks of operating on the Internet and the new techniques and technologies that can enhance Internet operations is imperative if we are to reclaim the Internet territory as our own.

The necessity for advanced technologies that enable military Internet operations has never been greater. Whether organizations are infiltrating terrorist networks or gathering intelligence on the cyber warfare tactics of nation-states, they must have secure, unfettered access to their targets.

### **Best Practices for Secure Internet Operations**

This presentation will begin with a brief overview of the everyday challenges that organizations face as they gather intelligence and try to infiltrate enemy networks. Attendees will learn about secure state-of-the-art non-attribution technologies and best practices that can be used to enhance and secure online investigations. In addition, real world applications for cyber warfare and other operations will be discussed. Any organization that routinely conducts online investigations will leave with a better understanding of how technological advancements can be adapted to the following types of operations:

**Research, targeting, and recruitment-** Intelligence gathering and recruitment of assets on the Internet are critical components for organizations. Analysts must be able to collect reliable open source intelligence (OSINT) and communicate securely.

**Large scale OSINT collection-** The ability to harvest and index large amounts of data is imperative to Internet operations. These activities can leave a very large footprint; hence special precautionary measures are necessary to ensure that these activities are not exposed.

**Persistent and managed alias identities-** Operators must occasionally assume persistent and managed alias identities online. Remaining secure in these types of operations is imperative.

**Asset/Informant communications-** Gaining intelligence from trusted assets and informants in remote parts of the world is a critical component in conducting warfare. Assets/Informants need to be able to safely communicate with their handlers, even under active scrutiny.

**Title:** Developing secure and resilient next generation communications networks supporting critical multi-media services

**Abstract Text:** Networks are constantly changing in terms of technology, services, architectures, access configurations and business models. The primary security goals for protecting critical infrastructures have typically been:

- *Protection of the network* refers to measures taken to increase its resistance to attacks that might partially or totally incapacitate it, and to prevent disclosure of sensitive information that might make it vulnerable to privacy violations and fraud. The access, perimeter, and core network layers need to be secured by addressing the network systems (e.g., routers, gateways), management processes, and the routing and addressing supporting structures.
- *Protection of user services* refers to measures taken to protect the application software, user interfaces (e.g., web-based), directories, proxies, and interfaces to legacy systems. Protection of services is, of course, tied to protection of the network itself and the supporting network services. This can be expanded to include different types of services (e.g., VPNs, Voice over IP), technologies (e.g., MPLS), and access configurations (e.g., Internet, Wireless).
- *Protection of data* refers to steps taken to preserve the confidentiality and integrity of the data traversing the network. Protection of the data is probably the paramount concern of the network's users, so it is imperative that the measures taken to protect the data be robust and end-to-end.

To apply this approach to a given infrastructure supporting multi-media services has been challenging. Security technology has been applied in a piecemeal fashion. Security needs to address additional dimensions including end-to-end service flows, intelligent user devices residing on different platforms, signaling, risks from internal and external entities, etc.. The infrastructure has to adopt some of the resiliency traits of the public switched telecommunication network to combat increasing cyber threats.

This presentation will describe the technical and operational challenges and risks arising from these different types of service models supported by Information Technology and communication technologies. It will also present a risk management model for addressing the threats and vulnerabilities as they are identified and become targets of intruders.