Multi-layered Security Approaches for a Modular Open Network Architecture-based Satellite

Brandon Shirley, Quinn Young, Peter Wegner, Jacob Christensen
Space Dynamics Laboratory
1695 North Research Park Way, North Logan, UT 84341; (435) 994-9165
Brandon.Shirley@sdl.usu.edu

Jeffrey Janicik
Innoflight
9985 Pacific Heights Blvd. Suite 250 San Diego, CA 92121; (858) 332-0970
JJanicik@innoflight.com

ABSTRACT

A growing trend in satellite development includes shortening the development lifecycle for hardware and software, cost reduction, and promoting reuse for future missions. Department of Defense (DoD) acquisition policies mandate system providers use Open Systems Architecture (OSA) where feasible. Modular Open Network Architecture (MONA) is a subset of OSA and paves the way to achieve cost reduction and reuse during a reduced development lifecycle. MONA approaches provide opportunities to enhance data security handling, including multi-layered security approaches, data monitoring, and logging.

Traditional satellite architectures use non-networked point-to-point communication and rely on radio communication security (COMSEC) for protection. This single layer of defense is an effective gatekeeper, providing perimeter security for any data transferred between the satellite and ground, especially if adapted to network data transfer protocols which integrate with spacecraft data architecture. However, a satellite designed using MONA can provide more tools for enhancing data security.

This paper explores the benefits of using a MONA approach for spacecraft, difficulties in implementing and securing such an architecture, and discusses possibilities for addressing security concerns in a MONA satellite through a multi-layer security framework. Ultimately, MONA provides a feasible path forward for realizing a modern security approach in satellite operations.

INTRODUCTION

Department of Defense (DoD) acquisition policy requires that system providers use Open System Architecture (OSA) where feasible.[1] The transition of satellite architectures toward OSA provides significant opportunities for enhancing data security. Many options exist for increasing space system security via OSA and several of these options borrow from the systems and practices that are already employed by terrestrial systems.

The overarching goal of utilizing OSA is to reduce the cost to develop, maintain, and update systems.[2] This goal is directly in line with the trend in satellite development toward reduced cost and increased reusability while adhering to tighter development timelines. Examples of this trend include Northrop Grumman's Modular Space Vehicle Bus (MSV), Space and Missile Systems Center's Standard Network Adapter for Payloads, North American Space Agency's Core Flight Software System, and Air Force Research Laboratory's Space Plug-and-play Architecture.[3,4,5,6] Reduced budgets and an increasingly competitive market are fueling this trend.

Modular Open Network Architecture (MONA), a term coined by the Space and Missile Systems Center (SMC), is a subset of OSA that implies the architecture is designed natively for net-centric data transfer. MONA paves the way for systems engineers to achieve the goal of cost reduction and reuse in shorter timeframes. MONA approaches are widely used in terrestrial applications because of improved interoperability, portability, and reuse when implemented in a model similar to the Open System Interface (OSI) model.[7]

This paper will discuss the benefits of shifting to an open system architecture, the additional benefits of a modular open network architecture, security benefits and challenges, and methods for implementing security within a MONA spacecraft.

THE SHIFT TO OSA

The space industry has largely depended on highly integrated spacecraft architectures to provide the sophisticated, high-performance systems needed for national and commercial space missions. The desire for ever increasing performance with very low production volumes over generations of space development programs has relied on customized, often proprietary, methods more akin to a craft or artisan process than the manufacturing processes of other industries. The maturity of manufacturing processes, open system architecture, and an increased understanding of how to apply approaches to low-volume production is spreading into the aerospace community.

The current era of space systems development is increasingly constrained by reduced budgets, design and development lifecycles, maintenance allowances, integration and testing timelines, etc.; in an effort to address budget constraints every aspect of space system design and development is condensed or reduced. The DoD is trying to address these constraints by achieving greater spending efficiency and productivity while optimizing system performance and reducing total ownership costs.[8,2] The DoD has recognized that closed, proprietary systems design is limiting competitiveness, is not as effective at fostering innovation, is less cost-effective or schedule-effective, does not ease integration, does not reduce cost of ownership, and is generally reaching a point that it is unsustainable. Although the current process produces highly capable systems that have been successful in producing space dominance for decades, they are achieved at a high cost.[9,10,11]

The desire of the customer base to reduce costs and increase benefits is providing the incentive needed to motivate a shift in business practices; however, there is still much work to be done to transition to a new architecture class.

Reducing development timelines and development costs can help with secondary concerns as well. Parts and technology obsolescence can be attributed to long development times of the entire system, which can sometimes take a decade; to individual component development timelines; and to an inability to easily retrofit new components into existing programs.

As the customer base continues to move toward modular, open architectures, they are discovering more advantages and showing stronger interest in overcoming weaknesses in traditional architectures.

The weakness of traditional architectures can be addressed by:[12]

1) Mandating open standards and protocols
2) Utilizing open interfaces to enable interoperability
3) Adhering to open interface specifications as system components are designed
4) Adopting adaptable, upgradable, and reconfigurable system architecture
5) Considering modular and open systems design benefits and concerns
6) Utilizing business strategies to gain access to competitive sources of supply and effectively manage technological obsolescence

This set of criteria can be boiled down to the need to increase competition, increase innovation, develop rapidly, reduce overall cost, increase reuse, increase interoperability, increase portability, and increase ease of integration. All of these needs can by addressed by using open system architecture.

OSA Background

When utilized correctly, OSA facilitates reuse, interoperability, and portability. OSA facilitates increased competition, reduced life-cycle costs, increased innovation, reduced schedule, faster and less costly repairs and upgrades, and enhanced interoperability as depicted in Figure 1.[13]

MONA achieves all the benefits of OSA and operates under a paradigm many developers are already used to, the Internet.

Ultimately, the adoption of OSA and MONA is spreading, and new advances in technology and systems engineering will help to expedite this process. MONA allows systems engineers to integrate commercial off-the-shelf (COTS) components with more ease, readily realize the benefits of hardware and software interface standardization, and readily realize the benefits of layered architectures. All of these benefits of MONA enable reuse, new technology integration, interoperability, portability, cost, and schedule reduction. These benefits and their subsequent effects create a strong argument for the utilization of MONA in space systems. However, MONA is not without its drawbacks. The next section will introduce the security benefits and challenges that come with having a space system made up of networked components.

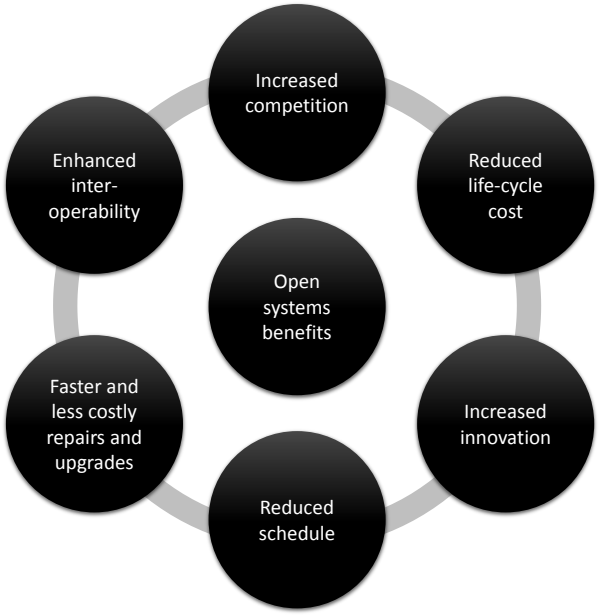

Figure 1: Open System Benefits*

SECURITY WITHIN A MONA SPACECRAFT

Most satellites today use non-networked point-to-point communication and rely on radio communications security (COMSEC) to protect the satellite. In this type of implementation, the entire spacecraft bus and all communication inside the security perimeter created by the encrypted radio system are trusted. A spacecraft incorporating MONA can have the same security perimeter, but with additional challenges and benefits.

There are many options for addressing MONA security and several borrow from the best practices employed by terrestrial systems. An ideal system would implement measures to protect space systems at the component level while minimizing the cost to assess and authorize a space vehicle.

Networked space systems can enable a paradigm shift toward the types of security policies and practices common for terrestrial networks. Extending the National Institute of Standards and Technology (NIST) Risk Management framework (RMF) into the space vehicle would provide higher levels of security and improved tools for implementing, monitoring, and evaluating the security. The RMF process includes risk framing, risk assessment, risk response, and risk monitoring.[14] The ability to monitor data traffic within the network and respond is an important part of risk management that could be implemented in MONA spacecraft.

MONA spacecraft approaches also result in some challenges from a security perspective. Networked systems enable data to flow easily from one part of the system to another. One challenge is to ensure that the data flow is intended, and not malicious. This challenge becomes more significant in broader networks, such as a hosted payload or networked satellite-to-satellite communications. Similar to computer systems linked by the internet, ensuring that a compromise in one part of the network does not propagate to other parts of the network is a security interest.

Security Challenges

The utilization of a MONA brings a set of challenges similar to those seen on the Internet, which is itself conceptually a MONA system. These challenges can be categorized as:

1. Access Control – Identify who is authorized to use the resources on the network and who is not, so that the system can respond appropriately

2. Auditing – Monitoring the network to ensure only those authorized to have access to certain resources actually have access, and keeping those who should not have access locked out

3. Response – The network response to unauthorized network communication

4. Adaptability – The ability to upgrade as risks to security are identified and solutions are found

Access control has many implications and the upcoming Security Principles section covers it in more depth. Figure 2 depicts a scenario that exemplifies the issues that can be encountered without access control. The desired communication traces are shown in green, while the undesired or unwanted communication traces are shown in orange. This diagram illustrates the issues that arise when there is no access control mechanism in place: there is no way to discriminate between desired and undesired traffic. This example only shows traffic initiated from external sources, but traffic initiated from internal sources has the same problem.

Auditing is critical to detecting attacks or abnormal behavior and troubleshooting problems. Figure 2 shows

*Source: GAO analysis of DoD and industry data.

that it is impossible in this system to identify who is communicating with whom, and this is especially true for internal only traffic. Even if measures are implemented to control access, there is no current means to determine how well the measures were working.

Response is associated with detection and mitigation. Detection ties into the Auditing component but also the need to characterize normal behavior, i.e. should these two systems be talking and at what rate. Unauthorized traffic should not be utilizing bandwidth or reducing a system's availability. Ideally, the network system could network flow information to detect malicious behavior and react appropriately.

Adaptability is a complicated issue. It includes the ability to update the rules and potentially some of the software infrastructure of a deployed system, upgrading hardware and software for a new mission, and updating hardware firmware after deployment. These are complicated issues and beyond the scope of this paper, but are mentioned briefly in the upcoming Supply Chain section.

Security Solutions

Networking the components of a space system enables the use of terrestrial network security solutions for controlling access and negotiating communication. A network also provides a medium for auditing communication and events. Having a networked set of nodes means that commercial, open-source, and industry best-practice security solutions can be adapted for space systems. This means additional layers of protection to a perimeter defense mechanism can be added.

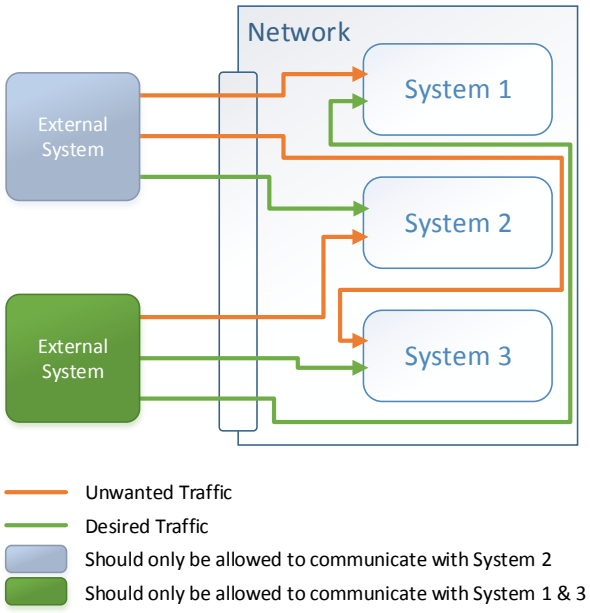

Figure 2: External Access Control Problem Example

Security Principles

At a basic level, networked systems need to be protected and network resources need access control through controlling traffic from external sources (Figure 3) and internal sources (Figure 4). Access control can get very complicated and the examples do not illustrate all communication patterns or policies that could be applicable for the example networks. The basic concept of access control has many implications. Providing for the security principles established in the NISTIR 7628 Guidelines allows the achievement of access control:[15]

1. Identity Management – In order to establish who needs to or gets to talk, a method for establishing identity is required

2. Mutual Authentication – Once identity is established, both communication systems need to authenticate the identity of each other

3. Authorization – Now that the systems have been authenticated, there needs to be a mechanism for determining the permissions for each system

4. Auditing – Tracking pertinent events for troubleshooting system issues and for detecting unauthorized behavior is desired

5. Confidentiality – A network is a shared medium and needs to ensure the conversations between systems are private, otherwise controlling access has little effect

6. Integrity – A network needs to ensure the conversations between systems are not being altered or otherwise subverted in transit

7. Availability – Systems need to be available when they are expected to be available in order to provide access

Principles 1 through 3 are concerned with securely and confidently verifying the identity of both parties that wish to communicate, thus ensuring that access is only provided to the intended party. Principles 5 and 6 deal with securely communicating in order to ensure that access is provided only to the intended party and that the access provided is not being tampered with. This is typically provided by an encryption scheme.

So how are these principles achieved? The security solutions for information technology (IT) access control are very mature and the security concepts and solutions for systems with similar constraints, like Smart Grids, are rapidly maturing. Space systems engineers have a wealth of tools from which to pull and adapt.

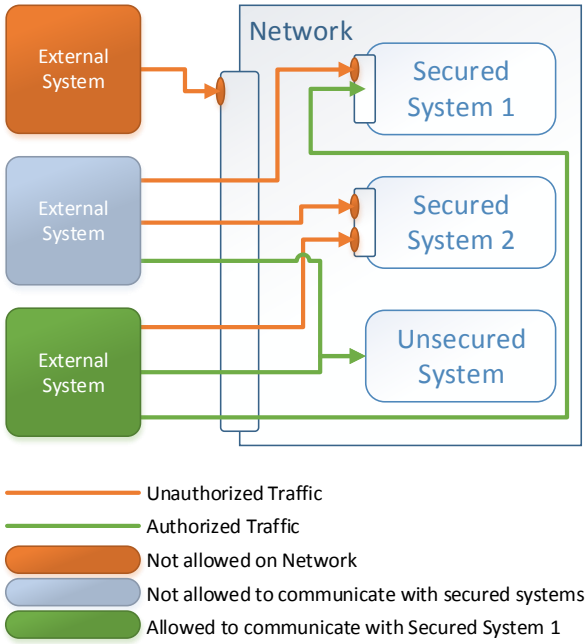

Figure 3: External Access Control Example

One more piece to the puzzle needs to be added: in a networked system, it is important to track what transactions are taking place, authorized and unauthorized. Figure 5 illustrates logging at a basic level. The same modules used to control access to the system and network can relay transaction information to the Logger. These modules would need to be trusted completely or a framework would need to be in place to determine the truth of a module's report. Another option would be to make the Logger part of the network fabric so that all transaction could be easily audited without any action from the end systems.

Establishing secure channels between the Logger and networks systems ensures the accuracy of the audit. Securing a network at fundamental levels means controlling access to the system's information and services while providing an audit trail for the transactions that occur on that network. Therefore, a mechanism is needed for identifying systems, authenticating systems, authorizing systems, auditing systems, communicating securely between systems, and ensuring the availability of systems on a network.

Solutions

The intention of the ideas expressed in this section is to provide a starting point for realizing MONA as a secure solution for space systems architecture. The key here is to maintain as many MONA benefits as possible when implementing an access control solution.

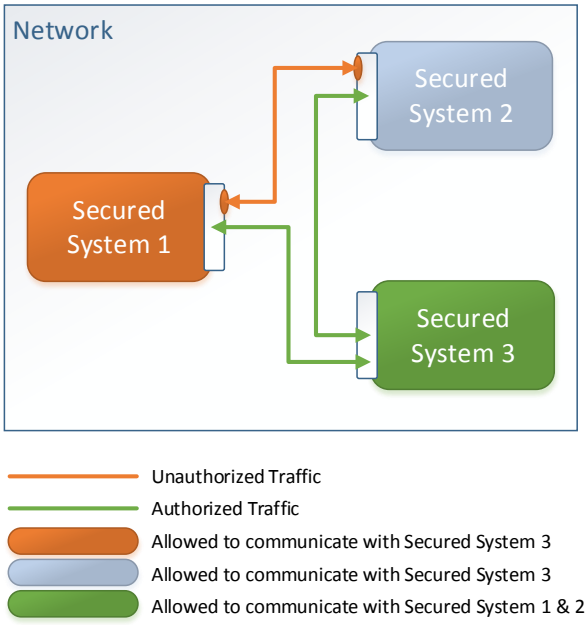

Figure 4: Internal Access Control Example

There are two typical approaches for implementing an access control solution:

1. Distributed – The ability to negotiate access lies strictly within the network nodes

2. Centralized – Access control is regulated by a central trusted authority

Both approaches have their merits; typically, the centralized approach will be the easiest to manage and will be the most adaptable in the face of network system changes.

Distributed Solutions

A simple example of a strictly distributed access control system would be discretionary access control (DAC). In this approach, the system that produces the data or accepts input also controls what other systems can request or supply it. This type of solution utilizes Access Control Lists (ACLs) within each system. These ACLs are essentially whitelists that prescribe a set of systems that the system will allow to communicate with itself. This alone does not provide authentication nor does it entail a mechanism for protecting data or input in transit. Each ACL system entry would need to contain secret information about the system. This information could then be used to authenticate the system and securely communicate with it.

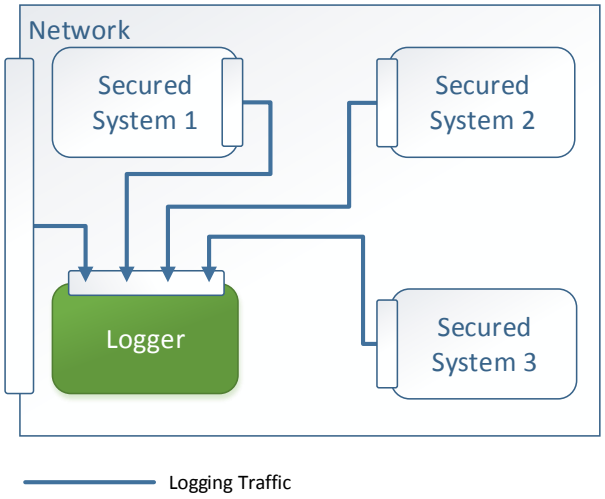

Figure 5: Network Logging Example

Assuming identity can be securely established and systems authenticated, DAC could, when coupled with an auditing system, provide for the principles discussed. Issues arise when components are replaced, new components are added, or when granular access control is needed. Adding new systems or replacing existing system means updating the ACLs of any systems that interacted with the replaced systems or that will interact with the new systems. This can be cumbersome to manage while building network in an offline state, but can prove quite difficult if the network is deployed and would require special out-of-band handling. Secret management is further complicated when system to service/interface is not a one-to-one relation, i.e. a system has more than one service or interface to which it must control access.

In general, these are management problems where secrets must stored for each system or, if the systems needs greater granularity, for each interface or service within a system. This is a typical problem with a truly distributed system, not just DAC. There still must be a way to update access control policy and secrets, but it is difficult to do this without a centralized management system.

Centralized Solutions

In a centralized solution, the network specifies and manages access from a central location. An example of longstanding centralized authentication and authorization system is Kerberos.[16] Kerberos utilizes a centralized Key Distribution Center (KDC) that must be secure and reliable since is poses a single point of failure. This issue can be minimized using replication, but other security provisions may be necessary to protect the overall functionality of the network. The Authentication Server (AS) and the Ticket Granting Server (TGS) comprise the Key Distribution Center. These two services, together with secret information stored on the system that wishes to authenticate itself, allow said system to establish itself as its claimed identity and, with the help of some other protocols, get access to the services on the network to which it has the proper permissions. The KDC is able to achieve this using symmetric key cryptography. Kerberos now allows for the use of public key cryptography during certain phases of the authentication process.

Networked components in a space system could use an authentication system like Kerberos to mutually authenticate themselves to each other and ultimately securely communicate. Another benefit of this type of centralized system is that the identity of who has sessions open with whom is known; this means that resource utilization can be tracked on a per system basis.

What other industries are utilizing for the security of their point-to-point systems as they transition them to networked systems should also be researched. A prime example of an industry that is undergoing this transition is the energy industry with its grid environments. The White House Networking and Information Technology Research and Development (NITRD) Program and the Department of Energy (DoE) developed a tailored trustworthy space (TTS) strategy for securing Smart Grids. "A trustworthy space is an isolated collection of devices, services, policies, and data that are meant to interact in a secure, private, and reliable fashion. Tailored indicates the need for handling the multiplicity of situations that comprise an end-to-end system and a need to use design patterns in different combinations to be able to mass customize appropriate solutions for the different circumstances common to the intelligent grid."[17]

There are some differences between space systems and intelligent grid systems that should be considered when adopting this type of strategy. Another point to remember is that TTS is a strategy and not an actual implementation. McAffee's, an Intel company, led a trail-blazing effort called Security Fabric for an actual implementation of the TTS strategy. This implementation meets all the security principles discussed so far, as well as a couple of others: identity management, authentication, access management, authorization, auditing, confidentiality, integrity, availability, non-reputability, and provenance.[17] The system supports secure controller and device node interaction via a set of services and logging capability as well some specialized hardware and software at the end systems. The concepts of TTS have applicability to space systems and Security Fabric shows those concepts can be tailored to a specific application. Undergoing a similar process for networked space systems would be a viable path forward to realizing secure networked space systems.

Another critical security component to consider are the integrity and confidentiality, or encryption, schemes or protocols that are already designed for networks. An example of such a protocol is IPsec. IPsec allows for mutual authentication as well as session key negotiation. IPsec provides for a lot of the principles discussed. If coupled with other security components, it could also provide for auditing or provenance. IPsec can allow for secure communication between end systems, network to end system or end system to end system.

Adding More Layers

Additional layers can be added to a security system by introducing additional protection mechanisms. An example of this might be network segmentation; Figure 6 illustrates the concept of network segmentation. Network segmentation allows greater separation between networked systems that should not be talking to each other.

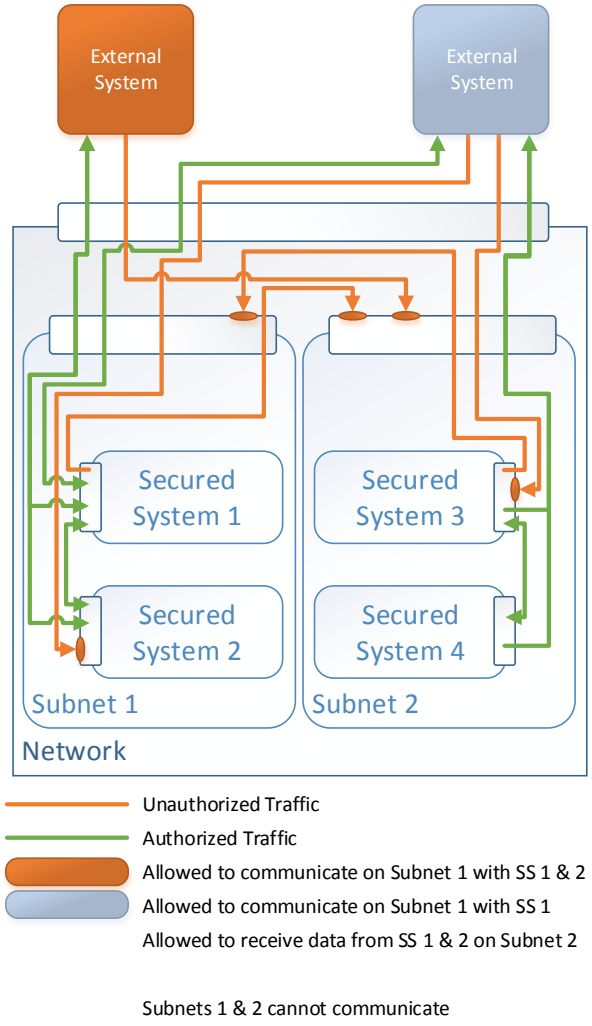

Figure 6: Network Segmentation Example

Supply Chain

Identity and authentication have thus far been discussed without relating what identity means, or how it might be established and trusted. This points to a more systemic issue of trust and ultimately provenance, or origin. So much needs to be known about the hardware and software that will be used in space systems in order to ultimately trust the data that is being produced; this is not a network-only challenge. System engineers, designers, and procurement personal probably already pay a lot of attention to this, but special consideration should be made as components become more complex in capability and sourcing. Multiple different manufacturers, designers, software firms, etc. will likely come together to produce a single COTS component and anyone in that chain could introduce a security problem, intentionally or unintentionally, into the overall product. The supply chain and testing procedures are as important as the security measures that will be put in place to protect the networks.

Maintaining OSA Principles

This paper has presented some of the information technology security solutions that might be tailored to the specific needs of a space system; there are many more that should be considered before deciding on the best solution. The best solution might ultimately be different, depending on the usage scenario. It would be advantageous, and in line with OSA principles, for the space industry to develop a set of standardized security architectures and processes for ensuring that a system is secure. The ongoing Space Universal Modular Architecture (SUMO) effort should be followed as an example, as it is trying to standardize and modularize all aspects of space systems, security included, as an example for how space security systems might be handled in an open systems architecture sort of way.

CONCLUSION

Economic and technological factors are driving space systems design towards OSA; MONA is a network centric OSA with which many developers are already familiar. MONA has all the benefits of OSA but also adds the benefit of networked systems. Networked systems come with a set of security challenges, but have been in place for a long time and there is a wealth of security tools that can be adapted to the special needs of networked space systems. Other industries, such as the energy industry, can be looked to for examples of how current network security technology can be tailored to address the special constraints of space systems.

Networked systems make sense from a cost standpoint and with the right provisions in place, they will also make sense from a security standpoint.

REFERENCES

1. Department of Defense. "Open Systems Architecture Contract Guidebook for Program Managers." Version 1.1, June 2013.
2. Department of Defense Directive 5000.01, "The Defense Acquisition System," May 12, 2003.
3. Cheng, Joey. "Northrop's Modular Space Vehicle gives Air Force faster satellite capability." Retrieved May 2014, http://defensesystems.com/articles/2014/03/03/msv-plug-and-play-satellite-northrop.aspx?admgarea=TC_DefenseIT
4. Ellis, Garrett. "SNAP: MONA's Foundation at SMC" Retrieved May 2014, http://gsaw.org/wp-content/uploads/2014/03/2014s11e_ellis.pdf, 2014.
5. Wilmot, Jonathan. "A core plug and play architecture for reusable flight software systems." Space Mission Challenges for Information Technology, 2006. SMC-IT 2006. Second IEEE International Conference on. IEEE, 2006.
6. Kief, C.J.; Zufelt, B.; Cannon, S.R.; Lyke, J.; Mee, J.K., "The advent of the PnP Cube satellite." Aerospace Conference, 2012 IEEE pp.1-5, March 2012.
7. ISO/IEC 7498-1:1994(E), Information technology– Open Systems Interconnection – Basic Reference Model: The Basic Model. ISO, Geneva, Switzerland, 2005. [Online]. Available: http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269 ISO IEC 7498-1 1994(E).zip
8. Office of the Under Secretary of Defense, Acquisition, Technology and Logistics Memorandum: "Better Buying Power 2.0: Continuing the Pursuit for Greater Efficiency and Productivity in Defense Spending" (Nov. 13, 2012).
9. [Fundamentals1994] Pisacane, V. L., and Moore, R. C., Eds. Fundamentals of Space Systems. Series in Science and Engineering. John Hopkins University Applied Physics Laboratory, 1994.
10. Messeri, L. R., and Richards, M. G. "Standards in the space industry: Looking back, looking forward." Management and Organizational History 4, 3 (August 2009), 281-297.
11. Leone, D. "Nasa: James webb telescope expected to cost $8.7 billion." Retrieved May 2014. http://www.spacenews.com/civil/110826-jwst-cost-billion.html.
12. [DoDInf] Office of the Deputy Assistant Secretary of Defense. "Systems Engineering Initiatives: Open Systems Architecture." Retrieved May 2014, http://www.acq.osd.mil/se/initiatives/init_osa.html
13. U.S. Government Accountability Office. "DOD Efforts to Adopt Open systems for Its Unmanned Aircraft Systems Have Progressed Slowly," GAO-13-651, July 2013.
14. National Institute of Standards and Technology, U.S. Department of Commerce "Managing Information Security Risk – Organization, Mission, and Information System View." March 2011, NIST SP 800-39.
15. National Institute of Standards and Technology, U.S. Department of Commerce "Guidelines for Smart Grid Cyber Security", August 2010, NISTIR 7628.
16. Kohl, John T., B. Clifford Neuman, and Y. Theodore. "The evolution of the Kerberos authentication service." (1994): 94
17. Integrated Architectures. (2011). "Security Fabric - an Implementation of the DOE Proposed Tailored Trustworthy Space." Retrieved from http://www.iai.com