Cyber-Security, Aerospace, and Secure Satellite Communications - Evolving our Approach

Mr. Jonathan Michael Mercado
Dr. Dale C Rowe, Brigham Young University

Dr. Rowe has worked for nearly two decades in security and network architecture with a variety of industries in international companies. He has provided secure enterprise architecture on both military and commercial satellite communications systems. He has also advised and trained both national and international governments on cyber-security. Since joining Brigham Young University in 2010, he has designed a variety of courses on Information Assurance, Cyber Security, Penetration Testing, Cyber Forensics and Systems Administration and published over a dozen papers in cyber-security.
Cyber-Security, Aerospace, and Secure Satellite Communications
– Evolving our Approach

Abstract: The satellite communications (satcoms) sector is a prime example of a complex aerospace cyber-physical system. To provide a secure, robust communications capability, satcoms systems are designed to implement defense in depth from targeted attacks and component failure as well as operate effectively in harsh environmental conditions. Due to the prohibitive cost of replacement, satcoms spacecraft are frequently designed with lifespans of over a decade and must provide a continual service – where any downtime is seen as unacceptable.

Recently, several international governments have developed cyber-strategies that go against the traditional ‘quarantine, resolve, remediate’ methodology. For example, the United States government now requires the continuation of operational capabilities as a priority – over and above that of the isolation and quarantine of systems that may be impacted in a cyber-attack. This new approach will require not only multiple levels of redundancy and a structured approach to cyber-defense, but multiple information and service pathways that use independent protocol and vendor pathways to provide ongoing operational capabilities.

While new cyber-strategies are requiring systems architects to rethink their approach to cyber-defense, there is actually no cause to re-invent the wheel. Effective lessons can be learned from a satcoms industry that has faced such requirements for many decades. Indeed, the Aerospace domain is, by its nature, required to produce systems that are designed to survive the simultaneous failure or attack of multiple components. For cyber-strategists and systems architects, this requires a shift in thinking away from the protection of information and towards the continuity of service.

In this paper, we present a methodology, adapted from aerospace practices, that facilitates the design of systems designed to provide continuity of service even while under attack. We also leverage established best practices in the cyber-security space and suggest enhancements to common methodologies found within the aerospace industry. For example, due to complex mission-critical requirements, legacy interoperability and multiple vendors, aerospace projects are frequently resistant to implement recommendations from penetration tests – as such changes require extensive retesting and validation. We believe, and demonstrate proof-of-concept, that our presented methodology will enhance both the resilience and security of traditional cyber-systems, as well as aerospace cyber-physical systems – and that this approach can minimize associated time, resource and cost expenses. We conclude our approach by the application of our methodology in various hypothetical, and tangible project architectures, and compare this to traditional approaches. As a final note we suggest that all industries in engineering and technology would benefit greatly from this cross-discipline approach to evaluating cyber-security early within the educational process.

Introduction
As we advance in the information age we are increasingly aware of the threat that cyber-terrorists pose to United States government and military networks around the world. In the past, information technology did little more for the government than to aid government offices in
administrative tasks, but has now become a critical part of military operations globally. The U.S. military cyberspace infrastructure is made up of tens of thousands of networks and millions of computing devices many of which are located internationally. Our forces need to be prepared to face ever-aggressive enemies in this new warfighting domain.

It has come to the attention of the international community that a proactive approach to protecting cyber assets is necessary, and many nations have published publicly available cyber-strategy documents outlining their approach to cyber-defense. U.S. executive order 13636 was given in February 2013 by President Barack Obama who addressed the need for “Improving Critical Infrastructure Cybersecurity” emphasizing the need for a collaborative and incentivized framework to be adopted in government and commercial entities understanding that we are severely underprepared for the threats that cyber-attacks pose to the United States of America. This framework was released in February 2014 and encourages the development of policies and procedures that, at their core, are built to identify, protect, detect, respond and recover from cyber-attacks.

While this framework addresses what needs to be done, it does not specify the techniques or technologies that should be implemented to realize its potential. We need to discuss how we can better approach cyber-defense to maintain national security. A fresh look at cyber-security practices is necessary as we evaluate recent attacks that have been realized against large corporate firms. In the past, response to a security breach often involved isolation of the effected system which was then cleaned, reimaged or otherwise recovered before introducing it back into production. In the meantime, a backup or redundant system took the load of the compromised system. This common solution may no longer be a sufficient incident response method as we move into the future.

In December 2014 Sony Pictures Entertainment (SPE) was attacked by a hacking group who identified themselves as the “Guardians of Peace”. This organization was confirmed by the Federal Bureau of Investigations (FBI) to be associated with the North Korean government. Given this and other state sponsored attacks that have occurred within the last several years, we can project that state-driven cyber war is likely in the near future. Given the nature of the Sony attack we can see how a ‘quarantine, resolve, remediate’ approach to recovery from cyber-attacks would be ineffective. According to the FBI press release given December 19, 2014, not only was a large amount of sensitive data stolen from SPE but, “The attacks also rendered thousands of SPE’s computers inoperable, forced SPE to take its entire computer network offline, and significantly disrupted the company’s business operations.”

Attackers have proven that they have the capability to perform large-scale operations against high-profile targets. With these capabilities it is not feasible to assume that a plan to quarantine compromised systems in wake of a cyber-attack while maintaining service availability will be a possible recovery method in the future. We must find ways to maximize availability of services even in the midst of a cyber-attack.

The understanding that we need a more robust cyber-strategy with an emphasis on maximizing availability is not new. In 2010 General Charles Shugg, vice commander of the 24th Air Force
unit stated, “We want to make sure cyber is integrated into the operational planning process from the beginning. We’ve got to learn how to fight through cyber-attacks.” 6

Given this requirement to maintain continuity of service in the midst of cyber-attacks, efforts are being made to adopt new practices that will allow us the resilience necessary to achieve this goal. However, in our search for cyber-security best practices for availability we do not need to re-invent the wheel. In the following sections we will discuss how effective lessons can be learned from the satellite communications industry which has faced such requirements for many decades. By applying practices adopted by the aerospace industry, we will develop a methodology for cyber-strategists and system architects to make availability a priority over the protection of information and in the end be more effective at achieving both. Our goal is to think outside the box of current cyber-security practices by considering satellite design and defense mechanisms. These will contribute to our cyber defense strategy so that we may become more effective in implementing a new cyber-security methodology.

**Satellites as a Cyber-Physical System**

Satellite communications (SatCom) technology has existed for almost as long as electronic computing. These complex cyber-physical systems are not the most commonly understood network devices within the Information Technology (IT) domain, but they have evolved an adapted over many decades just as other IT Systems. The aerospace industry has had to develop secure and robust methods of protecting their resources from physical harm as well as cyber-attacks. Due to the inability to perform hardware maintenance on deployed satellites, designing and implementing robust systems is key to maintaining availability and service continuity. It is from this legacy of satellite design that we can discover and implement strategies to be applied in other cyber systems.

It should also be understood, however, that a great deal of our satellite systems infrastructure is being integrated into the backbone of the Internet and communicating using protocols familiar to IT professionals. We now have television, phone, GPS and internet services provided via satellite links. In addition, ground stations which are crucial to the relaying of satellite signals to their proper destinations are also connected to the internet. This integration of technologies is driving satellite networks into the broader global network of systems which puts them at risk of attack from external entities. Unless cyber-security professionals are willing to take on the responsibility of assimilating these networks into their cyber-security risk assessments satellite links may become a great weakness in our ability to stave off cyber-attacks. We believe that our presented methodology will enhance both the resilience and security of traditional cyber-systems as well as aerospace cyber-physical systems thus evolving our over-arching cyber-security approach.

**Satellite Defense-in-Depth Design Strategy**

“Defense-in-depth” is a strategy that existed well before the information age. In the medieval era castles were constructed that were surrounded by moats and outer walls with watch towers constructed to provide multiple levels of defense for the inhabitants inside. The principles of implementing layered and multiple defenses have also been widely recognized as a best-practices approach to keeping IT infrastructure secure from cyber threat 7. However, security in this fashion is often an afterthought in cyber-systems design where business purpose and cost are
higher priorities. It is not possible to correctly implement a defense-in-depth strategy in this manner. Imagine the creation of a village where the priority is placed on maximizing farmland availability and housing for villagers. If the security of the village is not taken into account before the construction process, watch towers could not be placed in optimal locations where houses and farms occupied the land. Moats and outer walls may be shortened, narrowed or incomplete because of lack of monetary resources or perhaps left out altogether because of unbuildable terrain. Similarly, in IT systems, it is very costly to implement defense-in-depth after the infrastructure is established. Penetration tests that are performed on established infrastructure can reveal vulnerabilities in cyber systems but can ultimately lead to patchwork solutions that attempt to cover larger issues inherent in their initial design and implementation. Again, it being prohibitively costly to redesign and implement a working solution, security considerations must be introduced at the design stage of the cyber systems lifecycle.

Admittedly, this proposition can be much more easily said than done. With an increasing number of proprietary and open-source technology solutions that must work together to provide services, compatibility can be difficult to achieve. Considering a defense-in-depth strategy to security can become complex and costly. Let us take a look at a satellite design process that can mitigate some of these concerns.

**Satcom Design Strategy and Lifecycle**
The lifecycle of SatComs begins with a design process which is able to streamline the integration of components from multiple vendors required to fulfill complex mission-critical requirements.

**Preliminary Design**
This stage marks the start of system modeling which is fleshed out as teams discuss possibilities and options available to meet project requirements. Importantly, interfacing between subsystems is discussed and reviewed. Security concerns should be raised at this point as contingency scenarios are considered so as to maximize service availability under any circumstance. The entire lifecycle of the system is discussed at this stage understanding that its mission could last a decade or longer.

**Critical Design**
At this point plans for spacecraft construction and other subsystems are finalized and documented. Before construction of components begins, security considerations have been fully implemented and risk assessments have been performed to fully understand the implications of security hazards. This stage ends with a customer review in which project requirements, including security, are reviewed. If there are concerns with the design, the design is reviewed, adjusted and once again presented for customer review. This iterative design approach is present regardless of the development model utilized to manage the satcom lifecycle.

**Component and Interface Testing**
As components are constructed they are tested independently to ensure proper functionality and implementation of the completed design. This stage is again reviewed by the customer to validate correct operation.
**Systems Integration and Integration Testing**
As each subsystem is confirmed to function according to outlined specifications, the subsystems are interfaced to complete a working SatCom system. Before delivery, the integrated product is tested for functionality. In addition, a penetration test is performed to validate that all security measures in place are operational. A customer review is held to finalize the construction process.  

**Satcom Lifecycle Lessons in IT**
Given the high cost of SatCom projects and the risks involved in spacecraft component failure, the reasons behind such a vigorous design, testing and analysis process throughout the system’s construction are evident. These same principles, applied to other IT systems, would maximize the lifetime of infrastructure as well as provide inherent defense-in-depth hardening from its conception.

As a simple example we can consider the development of a web application. In order to set up this service there are several components or subsystems that need to be considered. A web application requires a web server, database, network, operating system, and possibly framework, programming language or other software packages. In the design phase we can consider security in each of these subsystems and determine best practices for defending them individually before integrating them. If our design is engineered to span the lifetime of the entire project, we can anticipate future needs and determine the robustness required from the beginning. This increases security as we will not need to perform major infrastructure upgrades during operational phases of the web application’s lifecycle. This is helpful because such upgrades may not fit our initial security requirements or may introduce new security problems that need to be patched in the future.

**Improving upon the Satcom Lifecycle**
While we see the benefits of implementing SatCom lifecycle strategies into other IT systems, we wish to augment SatCom strategies in way that will benefit both the SatComs industry as well as the broader IT community.

**Penetration Testing**
As was mentioned before, a penetration test is conducted on a SatComs system after integration of subsystems has occurred. While this step should not be omitted, we suggest that each subsystem should have a penetration test performed before final integration. In fact, as components are constructed, penetration tests should be performed at the lowest level possible. This will verify the defense-in-depth strategy that was initially planned. The more subsystems and components present in a system, the more difficult it is to fully evaluate with penetration testing. Though many vulnerabilities may be discovered in a penetration test, there is no way to determine if all vulnerabilities have been identified. Breaking down the test to evaluate subsystems as they become operational will increase the thoroughness of the security evaluation.

Satellite system architects have historically been resistant to implement recommendations from penetration tests as such changes require extensive retesting and validation. Again, by reducing the scope of individual penetration tests these recommendations can be implemented less expensively as problems are caught early. This will reduce the cost of implementing a secure
Satcoms system and discourage implementing insecure systems. Similarly, an IT project in the subcomponent development stage is much more flexible to design changes that may need to be implemented as a result of penetration testing recommendations.

**Satcom Infrastructure**

In addition to the way satcoms are designed and deployed, the way their infrastructure is set up is by its nature more secure than typical cyber systems. There are various subsystems which work together to support the mission of the satcom. Each of these plays a specific role and is isolated where possible.

**Spacecraft**

The spacecraft is the unit responsible for supporting and protecting the payload which carries out the intended mission. It also holds other communications equipment for interaction with ground-based satellite control systems and payload control systems.

**Satellite Control Systems – SCS**

Satellite Control Systems (SCS) are responsible for the operation of the spacecraft. They oversee and manage propulsion, power, environmental and diagnostic controls. These components are often referred to as Telemetry, Tracking, and Command (TT&C) systems. TT&C is administered from ground stations which communicate to the spacecraft via Baseband Systems.

**Payload Control Systems – PCS**

Payload Control Systems (PCS) interact directly with satellite payloads. The payload specifically includes the equipment is required to fulfill the mission of the program. For example, in a commercial television transmission mission the payload would include the transponders necessary to relay television programming. The PCS oversees and manages the operation of the payload and ensures service availability.

**Baseband Systems – BBS**

Baseband Systems (BBS) include communications equipment not covered in previous subsystem descriptions and could include ground antennae, computer systems utilizing the payload and other communications hardware.

**Network Management Systems – NMS**

Network Management Systems maintain the security and availability of interconnected terrestrial networks where base stations and other equipment are involved.

The described subsystems are all critical to the completion of the satcom system as each fills an important role in its functionality. However, understanding that their roles are quite different, these subsystems are to remain isolated except where necessary to fulfill mission requirements. This isolation provides the best form of security from outside attackers. If there is little or no inter-network access between subsystems, then a cyber-attack is much less likely to succeed. This methodology also inherently provides multiple layers of security. If an attacker were able to circumvent the Network Management System and it were properly isolated from other subsystems, the attacker would still be unable to compromise the spacecraft because the PCS and
SCS subsystems would not be connected to base-station networks. This of course is the ideal solution and it is sometimes the case that such isolation is not possible given certain mission requirements. Where this isolation is not possible, single-point-of entry between networks is recommended.

**Redundant Systems**

Within the spacecraft lie the many mission critical components involved in its payload and other TT&C components necessary for proper operation. As these items cannot be replaced or physically repaired mid-mission, a great deal of consideration as to the implementation of such devices must be given if the satellite is to perform adequately throughout its lifecycle. To this end, parallel redundant systems are often implemented to aid in recovery from component failure. A figure that represents the relationship between the reliability of a component and overall system reliability is called a block diagram. We divide the spacecraft into onboard subsystems and create pathways that detail possible means by which a satellite’s mission can be achieved. The mission is successful if a pathway from one end of the diagram to the other is functional. A simple example is shown below:

![Figure 1 - A simple block diagram outlining subcomponent redundancy (Downey, 1970)](image)

In the above example, multiple service pathways allow for several component failures to occur while still maintaining service availability. Were component X and component Z2 to fail, components Y1 and Z1 would be available to complete the satellite’s mission. The described method is not a simple 1:1 redundancy approach. Also this redundancy strategy requires at least two (more likely three) components to fail before the service becomes unavailable.

Again, this ideal scenario is not always possible to achieve but striving for an optimal configuration of components increases our chances of success. In satellite architecture evaluation the availability of each spacecraft subsystem is carefully considered and the probability of component reliability (R) is measured. This allows for a mathematical model to be applied which predicts the probability of successful mission completion. The following diagram is a typical satellite feasibility block diagram.
Satcom Infrastructure Lessons in Information Technology

In a typical IT environment there are many components that function together to create a working solution. In addition, there are also many ways that these components can be interconnected. In a world where broader interconnectivity is often the simpler implementation method in IT projects we find much more open access between systems and services than is necessary. This trust between these services and the networks they are connected to creates multiple attack vectors for hackers to exploit. If we seek to isolate subsystems, allowing for single point of entry between these subsystems, we can create a defense-in-depth infrastructure that is much more resistant to attack.

While taking a painstaking mathematical approach to risk assessment of IT subsystem failure may not be the ideal approach, understanding the redundancy methods used in satellites can aid us in maintaining service availability even in the midst of a cyber-attack.

Let us examine the simple case of a web server with an associated database server. Unfortunately, there exist too many services in which the database and web servers are installed on the same machine (physical or virtual). This presents a single point of failure for our service and requires a ‘quarantine, resolve, remediate’ approach to system recovery if the machine is...
compromised by cyber-attack. The service must be taken offline in order to resolve either a database or web server breach. In this case the block diagram would appear as follows:

![Block Diagram](image)

**Figure 2 - Single point of failure block diagram**

In a well-planned scenario, IT infrastructure includes unique servers for subsystems and a backup system that is set to launch if primary systems become unavailable or are compromised. The primary and backup systems are isolated from one another which contributes to a defense-in-depth strategy. This is a much better solution, but requires that the entire primary system be taken offline if a subsystem is compromised or disabled. It is also not cost effective as the backup system has no useful purpose until the primary system fails:

![Block Diagram](image)

**Figure 3 - Redundant system block diagram**

In order to maximize service availability and reduce costs we can take the principle of multiple pathways from satcoms and apply it to our web application infrastructure in a meaningful way. We do this by enabling all available resources to support the desired services and allow each independent system to share subsystem resources should a component fail:

![Block Diagram](image)

**Figure 4 - Block diagram demonstrating multiple pathways**
Then, utilizing multiple isolated networks to add to our defense-in-depth strategy we can further protect our infrastructure through compartmentalization. We can do this any number of times dependent upon the amount of resources required to deliver services at optimal performance:

![Diagram of Isolated Multiple Pathways](image)

*Figure 5 - Isolated multiple pathways block diagram*

In this simple scenario we have applied and combined strategies used in the satcoms industry to create an IT environment that is secure, robust and maximizes availability. We call this an Isolated Multiple Pathways methodology for IT systems. The example we have examined is very simple as there are typically many more subcomponents and other network devices and infrastructure that are not considered here. However, we believe that this abstract perspective can have meaningful applied value in the design of many types of future IT systems providing various services.

It should be noted that each isolated network is identical with regard to function and services, however, there are security integration differences between each to make compromise of several networks less likely. For example, the usernames and passwords utilized in system A may differ from those in system B or the networks may be deployed in geographically different locations.

**Advantages of an isolated multiple pathways infrastructure**

The advantages to adopting this approach to IT infrastructure are as follows:

- Isolated networks harden against complete infrastructure compromise which allow services to remain active in the event of an otherwise catastrophic cyber-attack.
• Multiple service pathways allow for subsystems to fail without crippling system performance. Subsystems can be replaced while providing continuity of service.
• Cost effectiveness of Isolated Multiple Pathways is high because all infrastructure components are active at all times and able to contribute to the intended mission.
• Compartmentalization of networks helps protect against Distributed Denial of Service (DDOS) attacks.

Implications for IT Education
In this paper we have discussed the ways in which lessons learned from the aerospace and information technology industries can be mutually beneficial when applied to new or existing scenarios. Unfortunately, there are gaps in the education of students and professionals in bringing cyber-security to the forefront of their fields and applying it in effective ways. This is evidenced by a lack of attention to defending against cyber-attacks in new satellite networks where TCP/IP and other protocols familiar to IT professionals exist as well as the lack of communication between engineers with regard to constructing cyber-systems in the aerospace and information technology domains. As evidenced by the ideas presented in this paper, a great deal of progress can be made by bringing individuals together in closely related fields to innovate methods of defense that protect our critical and other infrastructure. If we do not, we put ourselves at risk as our world becomes more interconnected. Industries that once had little concern for attack in cyberspace must now become much more aware of the threats and devise defense strategies that best protect their assets.

In engineering and technology, cyber-security occupies only a small portion of the educational surface area that is considered in today’s curriculum. It is necessary that new technologies be developed with security in mind. Not only must security be considered at the forefront of infrastructure development but also at the start of innovation and invention. This means that our students must have the background necessary to be security aware and understand the possible risks associated with new technologies.

Conclusion
We have discussed ways in which the satcoms industry has approached satellite reliability and security and how these can be applied to other IT systems. Satellite System design and lifecycle processes can encourage IT professionals to consider security a priority alongside availability by performing multiple reviews, penetration testing subcomponents and carefully planning the entire lifecycle of infrastructure where possible. In addition, we discovered that satellite architects’ approach to spacecraft reliability can improve the security of our IT systems if we are able to utilize multiple service pathways in our production mechanisms. We have also emphasized the need to present security early in the education of our students in order to encourage a security mindset in new engineers and technologists.

The application of Isolated Multiple Pathways in the design process combined with subsystem and complete system penetration tests will differ depending on the project and will require validation in real-world scenarios. This provides ample opportunity for additional work to be performed in this area.