Making a Case for Hardening Aviation’s Cybersecurity System

By ATCA Cybersecurity Committee

With today’s increasing threats to computer and network systems, making systems resilient to attack is paramount. Implementing a cybersecurity policy requires hardening the system, including all sub-systems and components, against the potential risk of attack and exploitation of vulnerabilities with a budget that includes security for each system and expands the role of operations in its understanding of cyber risks. Once a comprehensive cybersecurity policy is accepted, hardening systems against potential risk is the crucial next step. With the increased complexity of system-of-system architectures based on Internet Protocol (IP), i.e. NextGen, it is becoming more important to cyber-harden systems and sub-systems to minimize vulnerabilities inherent in their software, firmware, and hardware.

Hardening is the process of identifying, analyzing, and remediating a system’s technical vulnerabilities to minimize exploitable weaknesses. It focuses on the need for concise but flexible security engineering processes that pave the way for “built-in” security controls that remediate known vulnerabilities. Following these engineering practices during all phases of system development ensures a groundwork is established for hardening a system. Implementing system hardening has its challenges – most notably the blending of security requirements into the budget process, the importance of security architecture, and the buy-in of senior management to integrated security.

For the aviation industry – FAA, airlines, pilots, air navigation service providers (ANSPs), airport authorities, and the private sector – budget is a main driver for their security posture. The federal government is embarking on a program to cyber-harden both developing and legacy systems to ensure that technology remains operational during a cyber attack. New legislation, executive orders, and department and agency initiatives are stimulating an increased focus on cybersecurity. This involves a myriad of activities: implementing security engineering at the earliest stage of a system’s lifecycle and securing software development practices, anti-tamper technologies, increased security testing, and supply chain security measures. All of these activities must be built into a system during its development, ensuring that security engineering activities do not interfere with NAS operations. All of this requires funding. As they stand now, budgets do not allow for cybersecurity control funding through a system’s lifecycle. Where budgets are concerned, cybersecurity is treated reactively instead of proactively; it’s the looming threat of a tidal wave before it crashes. No program exists to ensure funding of cyber common control, leaving a void in supporting security architecture across various systems.

Adding to the complexity of this challenge is inherited risk that comes from integrating aviation data to enable operational concepts such as Collaborative Trajectory Options Program (CTOP), which is a method for managing demand through constrained airspace and cutting down on congestion. As the aviation industry begins mitigating vulnerabilities in its own operational architecture, impacts
Cyber-hardening a system is all about changing mindsets, from a reactive to a proactive-focused approach.

are likely greater between ANSPs and industry stakeholders. The aviation industry should band together to form an overarching operationally secured architecture to ensure the inherent security risk is acceptable. A long-term budget strategy that allows for an integrated security architecture is necessary, thus facilitating an understanding of acceptable operational risk.

**Funding Cybersecurity in a System’s Lifecycle Budget**

In June 2016, a global study by Ponemon Institute showed businesses worldwide will wait for cyber attacks to occur before they take action. About two-thirds of the respondents said it took a large data loss to engage in proactive actions to prevent a cyber attack, with budget being the driving factor. The report, “Don’t Wait: The Evolution of Proactive Threat Hunting,” describes how that trend is changing and that companies are now looking for more from their technology providers. This report points out that traditionally managed security services (MSS) do not use advanced analytics, provide incident response, or mitigate threats, and they are typically not compliant with data protection requirements. Although many information security requirements are included in program scope, budgets are not based on the real world technical, administrative, testing, and review activities that will result in the fielding and operation of a truly secure system.

FAA program offices create system budgets based on the line operational evaluation (LOE) required to create a compliant system assessment resulting in an authorization package (A&A) that will allow for acceptable tactical and strategic risk. The A&A identifies vulnerabilities for which the program must create a plan of action and milestones (POA&M) to mitigate. As a result, system budgeting for cybersecurity control is driven by compliance, not a security risk management process, and the scope of cyber risk is limited to the definitions in FAA Order 1370.121, the National Institute of Standards and Technology (NIST) 800-53, and NIST 800-37. Programs operating in a budget- and schedule-constrained environment are therefore not incentivized to highlight additional cyber risks through periodic vulnerability scans, lifecycle reviews, increased security testing and analysis, or independent validations.

The FAA’s Joint Resource Council (JRC) is the primary board responsible for ensuring that system acquisitions and enhancements comply with the Acquisition Management System (AMS). The AMS serves as the roadmap that all programs must navigate to receive funding. The primary enforcement mechanism that the JRC uses to manage this process is the “JRC Checklist.” This checklist is used by program offices to determine the minimum acceptable set of documents and deliverables necessary to proceed through the various phases of the lifecycle.

One of the challenges with this process is that it does not include specific, comprehensive system security requirements in the early concept and design stages. The process does not ask for security to be part of a program, which means that it is often considered after the fact when it is significantly more expensive and difficult to implement. This is particularly true for operational mission critical systems. Designing security into the system’s original requirements is a more cost-effective and practical approach to ensure that the FAA is fielding systems that are highly secure. The current budget process also makes it very difficult for a program to retroactively ask for additional funding to mitigate security vulnerabilities discovered during routine security assessments.

According to the Ponemon Institute report, over 50 percent of company security leaders who relied on a support service were able to improve cybersecurity posture and not have to retain in-house top
talent or technology. Few companies are currently including cybersecurity as a budget line item.

An NAS-level set of security requirements is necessary. These requirements would include budget-related details to aid the program in estimating their security funding needs. To aid in this, the FAA can identify and appoint internal security engineers and subject matter experts to assist programs with the development and budgeting of their security-related requirements. In setting the security requirements, the FAA should look to existing models, such as the NIST Cybersecurity Framework (CSF) for guidance. The framework, which was created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure. In addition, the FAA should pursue representation on the Aviation Information Sharing and Analysis Center (A-ISAC), which facilitates collaboration across the global aviation industry to enhance our ability to prepare for an operational response to a successful cyber attack. It is necessary to have processes in place to respond to vulnerabilities, incidents, and threats; to disseminate timely and actionable information among member firms; and for A-ISAC to serve as the primary communications channel for the aviation industry with respect to such information.

System Architectures: Embedded Operational Security Updates in Real Time

System architectures should be designed with the assumption that there will be failures and intrusions. Therefore, they need the capability to detect intrusions and require redundant and distributed databases and processing to allow for safe contingency operations and rapid recovery from failures and malware. Cyber-hardening the global airspace is an impossible task. It’s made up of dozens of ANSPs, each with a complex system architecture. The FAA and the NAS are at the top of the list; its complexity is unrivaled, which only adds to its vulnerability.

As a means of ensuring the timely and accurate sharing of flight information for global ATM, a worldwide SWIM “service bus” is being developed. This allows all ANSPs and their subsidiary ATM systems to freely share the information required for efficient ATM. However, the level of trust for external ANSP SWIM domains will vary. Moreover, secure governance requires that each SWIM domain or information system has comprehensive data governance mechanisms for policy enforcement, as well as continuous security detection that monitors incoming and outgoing information for potential security threats and malware. Integrating an additional operational safeguard, such as CTOP, is necessary. CTOP helps balance airspace demand with available capacity, which aids the operational availability of the overall NAS system architecture.

Researchers D. Mu, W. Hu, B. Mao, and B. Ma, in their paper, “A Bottom-Up Approach to Verifiable Embedded System Information Flow Security,” researchers discuss the large deployment (as with NextGen and other FAA programs) of embedded systems. The constant rise in the systems’ interconnections increase the overall threat exposure. The authors discuss how the embedded systems are attacked through security holes that are more difficult to find with current or past assessment measures. Their argument is that “embedded security should be accounted for during the design phase from all abstraction levels with effective measures taken to prevent unintended interference between different system components caused by harmful flows of information.” In the NAS, this requires a budget that provides cradle-to-grave support. The study’s mindset and processes should be adopted by the FAA for its future budgetary decisions.

Authority to Operate (ATO): Approval Package Does Not Equal a Secure System

The FAA permits ATO by the assentance of risk. Per the Office of Management and Budget (OMB) Memorandum M-14-04, OMB identified cybersecurity as one of the top cross-agency priorities. OMB’s aim is to improve cybersecurity performance by focusing on what data and information are entering and exiting their networks, who is on their systems, and what components make up their information networks. It prioritizes (1) measuring agency implementation of trusted internet connections, (2) focusing on strong authentication through the use of multifactor authentication in accordance with Homeland Security Presidential Directive-12, and (3) monitoring security controls in federal information systems and environments in which those systems operate on a continuous basis.

OMB’s traditional reliance on three-year reauthorization of systems has been supplanted by the requirement for continuous monitoring with intrusion detection and vulnerability scanning, which involves an independent review of either an agency’s compliance team or a third party. The development and operation of complex NAS-based systems, however, present unique challenges. It’s not always possible to preemptively plan for cyber-hardening in each system’s budget. For example, security challenges (e.g. spoofing) present in systems such as Automatic Dependent Surveillance-Broadcast (ADS-B) may be the first of their kind, not covered by existing tools, and understood by only the most technical developers. In addition, not all of these issues are known at the time of system design; some are uncovered during development or operation. As a result, program offices cannot budget for their specific remediation during the JRC process and are not incentivized to emphasize third party validation of their

A Special Thank You to Our ATCA Cybersecurity Committee:

Chair:
Steve Carver, CSRA

Committee Members:
Mike Ball
Terrence Blair, Tetra Tech
Debbie Daniels, NGC
Gerry Hoff, Boeing
Steve Hoffman, USAF
Dennis McCallam, NGC
Bob Olsen, North Star Group, LLC
Jeff Snyder, Raytheon
Paul Storck, ARINC
Linda Weiland, ERAU

ATCA Staff Liaisons:
Kristen Knott
Paul Planzer
mitigation during program execution. Once A&A is satisfied (based on well-known vulnerabilities), the final ATO is signed Authorization Official, relying on the advice of the same program which developed the system. Per OMB M-14-04, annual testing of a system's information security practices should be required to help mitigate these challenges after the development and rollout of a system.

The processes recommended by NIST are a good step for understanding the security health of a system through a more frequent assessment of technical controls. However, the NAS does not have requirements for security monitoring. The lack of such a requirement has resulted in the inability of the NAS to analyze the security health of its systems in real time. Being a real-time safety environment, the NAS cannot be subjected to scanning or online changes unless such capabilities are required from the beginning of a system's development.

Additionally, operations should understand system health at all times. To achieve this understanding within operations, a clear picture needs to be provided as to how an effective cyber attack will manifest itself. This understanding will require a new way of thinking for most security experts. In the world of IT, operations is mostly about response from the user community when they experience slowdowns or if they are unable to assess an application. For NAS operations, there is no comparison. Interruptions to the flow of information that controllers need to make real-time safety decisions can lead to catastrophe in the sky or on the ground. Therefore, it is imperative that the security personnel be knowledgeable on potential system vulnerabilities and how they manifest themselves in day-to-day operations, and that these personnel then analyze the vulnerabilities to develop operational mitigations.

**Recommendations**

In light of the above challenges, the ATCA Cybersecurity Committee recommends that the FAA take the following multi-pronged approach:

- Prioritize NAS systems based on their impact to local and strategic operations.
- Allocate security-specific funding across the NAS based upon a prioritization of the systems.
- Identify internal security engineering experts who can assist programs with the development and budgeting of their security-related control requirements.
- Develop a NAS-level set of security requirements that can be provided to the implementing programs. These requirements would include budget-related details to aid the program in estimating their security funding needs.
- Develop NAS security requirements based upon existing frameworks such as the NIST CSF.
- The FAA, specifically its Air Traffic Organization (ATO), and the FAA Chief Information Security Officer, should have representatives on the board of the A-ISAC to encourage collaboration on cybersecurity risk.
- Require annual testing of system information security practices.
- Develop and incorporate operational mitigations based on the violations of security vulnerabilities that are known across all operational systems.

**Conclusion**

Cyber-hardening a system is all about changing mindsets, from a reactive to a proactive-focused approach. A budget that reflects the strategic cybersecurity risk across aviation needs to be developed within the ANSP as well as aviation operations in private industry. A long-term budget strategy that allows for aviation to integrate security architecture has never been more important than it is today. An NAS-level set of security requirements is fundamental to ensuring the continued safety of our nation’s airspace and aviation infrastructure. The current system architecture of the NAS isn’t equipped to handle a major cyber attack. The FAA should implement new security requirements using existing models and develop operational mitigations to help eliminate the impact of successful cyber attacks. There are many challenges and constraints going forward, but the time to act is now. No longer should aviation be limited in its capabilities to defeat the looming cyber threat that threatens to cause grave damage to the infrastructure and industry. In aviation, operations needs to be a mitigation factor for cyber attacks. We need a well-rounded capability against cyber attacks that include operational, technical, and managerial controls.

**References**

[1.] Dejun Mu, Wei Hu, Baolei Mao, and Bo Ma, “A bottom-up approach to verifiable embedded system information flow security,” The Institution of Engineering and Technology, Vol. 8, Issue 1, Jan. 2014.