

Information Systems Security

The Federal Aviation Administration's Layered Approach

DANIEL J. MEHAN

(This article first appeared in the November-December 2000 TR News, issue number 211)

The author is assistant administrator for information services and chief information officer for the Federal Aviation Administration.

The security of our nation, the viability of our economy, and the health and well being of our citizens rely on infrastructures for communication, finance, energy distribution, and transportation (1, p. 12). When these networked information systems are compromised, life and property are at risk.

The Federal Aviation Administration (FAA) develops, maintains, and operates one of the largest and most complex of these critical infrastructures; an infrastructure that is almost totally information centric. Destroying information or changing it improperly can disrupt the work of FAA and the national airspace system. The disclosure of sensitive information about ongoing, critical transportation functions to unauthorized entities can harm the operations of FAA and other government agencies.

For FAA, information systems security extends beyond the computer environment to the security of airspace and the national airspace system. The structural, operating, and procedural foundations of information systems security provide the mechanisms for achieving FAA's safety, security, and efficiency goals.

Directed Efforts

Presidential Decision Directive 63 (PDD-63) on critical infrastructure protection, signed in May 1998, called for a national effort to secure the increasingly vulnerable and interconnected infrastructures of the United States, including telecommunications, banking and finance, energy, transportation, and essential government services. The directive required immediate federal government action, including risk assessment and planning, to reduce exposure to attack and stressed cooperation with the private sector.

Although facing severe budget constraints in Fiscal Year (FY) 1999 and FY 2000, FAA has complied proactively with PDD-63. In February 1999, the agency hired its first chief information officer. In March 1999, FAA published its Critical Infrastructure Protection Plan, a mission statement for information systems security. Other efforts are under way both to protect the infrastructure and to ensure that new systems incorporate information systems security. These efforts include

- ◆ Certifying and authorizing systems,
- ◆ Training FAA personnel in security awareness and vulnerability assessment,
- ◆ Developing an information systems security strategy, and
- ◆ Establishing capability for immediate detection of intrusions.

FAA Order 1370.82, Information Systems Security, recently updated organizational and management responsibilities for implementing several earlier laws and policies, such as the Computer Security Act of 1987, taking into account the technological changes and challenges of the 21st century. Through presentations at the TRB Annual Meeting in January 2000, at the Computer Security and Information Assurance Conference in May 2000, and in meetings with the National Security Council and other government agencies, FAA has presented its approach and solicited input, as called for by PDD-63. FAA also has worked with the Office of Management and Budget, the White House, and Congress to ensure that the information systems security budget for FY 2001 reflects the sizable challenge.

The possibilities of new information technologies bode well for a healthy economy but also bring formidable security challenges to government and industry. Information systems security poses one of the most critical challenges to our nation in the first decade of the new millennium.

Complex Network

FAAs networked information systems are among the most complex in the world. The systems comprise

- ◆ Critical command and control capabilities essential to air traffic control;
- ◆ Complex weather and environmental networks essential for the safety and efficiency of air flight; and
- ◆ The essential operations of a large, geographically dispersed government agency.

Budget Sources

FAA has nearly 50,000 employees overseeing federal interests in a national airspace system of more than 3,000 public use airports. The agency's FY 2000 budget was nearly \$10 billion, provided through annual and multiyear appropriations by Congress. The largest appropriation is for operations, funding the salaries and associated costs of operating and maintaining the air traffic control (ATC) system and carrying out safety inspections and other regulatory and security responsibilities. The FAA budget also includes three capital investments:

- ◆ The facilities and equipment appropriation, which authorizes funds to modernize and expand the ATC systems;
- ◆ The Airport Improvement Program (AIP), which provides grants to expand and improve the nation's public use airports; and
- ◆ The research, engineering, and development appropriation, which provides funds to develop new aviation technology and systems.

FAAs FY 2000 budget included \$5.9 billion for operations, \$2.1 billion for facilities and equipment, \$1.9 billion for AIP grants and \$0.15 billion for research, engineering, and development (Figure 1). FAA's information systems security budget primarily comes from the budgets for operations and for facilities and equipment. A new research, engineering, and development program awaits Congressional approval.

Essential Safeguards

A recent General Accounting Office (GAO) report on aviation security stated:

Securing the ATC computer systems that provide information to controllers and flight crews is critical to the safe and expeditious movement of aircraft. Failure to adequately protect these systems, as well as the facilities that house them, could cause nationwide disruption of air traffic or even loss of life. Moreover, malicious attacks on computer systems are becoming

an increasing threat, and it is essential that the FAA ensure the integrity and availability of the ATC computer systems and protect them from unauthorized access. Numerous laws, as well as FAA's policy, require that these systems be adequately protected. (2, p. 4)

The protection of FAAs information systems begins by defining the primary security services required and then mapping these services appropriately to subsystems and facilities. Information systems security operations protect and defend through authentication and access control, maintaining integrity, confidentiality, and availability: FAA also plans to address additional security services such as nonrepudiation (see Glossary of Terms, page 10).

Holistic Approaches

Information systems security supports FAAs safety, security, and efficiency goals by enabling the development and operation of trustworthy systems. A trustworthy system performs only as expected, despite environmental disruptions, human or system errors, or hostile attacks. The system must avoid or eliminate design and implementation errors or must be so robust that potential errors can have no impact. Addressing only some of these dimensions or assembling trustworthy components is not sufficient—trustworthiness is holistic and multidimensional.

Information systems security is not a technical problem only but must be addressed through structural, operational, and process models:

- ◆ The structural model defines the layers of protection needed to safeguard FAA's information systems.
- ◆ The operational model details the facility and organizational relationships necessary for an effective and efficient security program.
- ◆ The process model explains the steps needed to develop and maintain trusted systems.

The following text describes the FAA's structural model for information systems security.

Layered Pyramid

The structural model provides the focus for information systems security efforts. The model can be depicted as a pyramid (Figure 2) with five reinforcing layers of protection:

- ◆ Personnel security,
- ◆ Physical security,

- ◆ Compartmentalization and information systems security,
- ◆ Site-specific adaptation, and
- ◆ Redundancy.

Some of these elements have been in place at FAA in response to other requirements. For example, redundancy ensures that no single point of failure causes an accident. Other elements are unique and new or are facing dramatic change. All five layers are necessary to maintain trustworthiness as FAA systems increase their interconnections in cyberspace.

Personnel Security

The top layer of the pyramid, personnel security, ensures that personnel with sensitive roles or access to sensitive information are trustworthy: Authorized personnel directly oversee the most sensitive FAA operations and contractors must have solid reputations in the industry. FAA personnel, contractors, and subcontractors must undergo appropriate background checks.

Several ongoing FAA initiatives, such as the integrated Capability Maturity Model, will ensure that FAAs acquisitions and operations follow best practices and hire contractors with solid experience to build, field, and operate reliable and trust-worthy systems (3). In addition, only authorized personnel will have access to information technology (IT) resources.

Physical Security

The second layer of the pyramid, physical security, ensures that FAA facilities are safe from unauthorized access and harm. Unescorted access in facilities is allowed only to authorized and screened personnel. FAA personnel must escort all other visitors within sensitive facilities.

In addition, critical elements of the infrastructure are located behind protected boundaries with a variety of barriers against intrusion. In sensitive locations, other detection and surveillance techniques increase security: The agency also is investigating several promising new technologies, including biometrics (iris scans and fingerprints) and smart key encryption devices, to ensure that only authorized personnel use the IT resources.

Compartmentalization and Information Systems Security

The third or middle layer of the protection pyramid, compartmentalization and information systems security, provides mechanisms to constrain and control the impact of any single security incident.

For example, FAAs ATC facilities are resilient because a security incident at one facility cannot spread to another. Each of the 20 centers that manage long-distance air traffic can operate independently. If one center is disabled, the other 19 would still operate.

The historically prevalent isolation of FAA computer systems—which aided compartmentalization—now is eroding as modernization and emerging information superhighways improve efficiency by closely interlinking systems. FAAs information systems security program must include electronic checkpoints and roadblocks to compensate for the loss of isolation.

Site-Specific Adaptation

The fourth layer of the structural model, site-specific adaptation, is the result of long-standing procedures at FAA. Each site uses its own specific "vanilla" code, adapted through a special database. The adaptation provides each facility with a unique "fingerprint" of airspace, geography, equipment, and procedures; makes each facility's ATC system work properly; and is critical to the information systems security structure.

The adaptation database must match the finger-print of each facility before a new ATC system can be installed. The process is labor-intensive and complex, requiring detailed understanding of a facility, but also makes it difficult for unauthorized personnel to insert bogus code into an ATC facility. To improve efficiency, however, this process must become simpler, faster, and more open, raising new security risks to address.

Redundancy

The final layer of the information systems security structural model is redundancy, a core element of the system design philosophy. Redundancy provides the robustness to ensure that FAA systems perform as expected. No single point of failure can keep FAA from operating and carrying out its mission, despite attempts to disrupt and alter code in the national airspace system. Multiple levels of redundancy protect the system so that FAA could perform its mission even if there were incidents of code tampering.

Primary, secondary, and manual mechanisms ensure that national airspace systems operate as safely and as efficiently as possible under adverse circumstances, allowing no compromise. Every critical system element has backups. Nonetheless, new and emerging threats can attack several systems simultaneously, taking more than one system off-line at the same time. FAA must address this kind of threat in part through increased redundancy in computing and communications.

Implementing Security

These five layers of protection constitute the front face of the information systems security pyramid. The right and left faces of the pyramid deal with awareness and execution and with architecture and engineering, respectively. These two themes apply to all layers of the pyramid.

Awareness and execution address the short- and intermediate-term implementation of information systems security, and architecture and engineering deal with longer-term aspects of implementation.

Awareness and Execution

Awareness and execution activities determine the vulnerabilities of information systems through assessments and penetration tests and establish strategies for countermeasures. Awareness also includes the operational training of system administrators and integrated product teams.

Virtually all FAA personnel have received security awareness training. In addition, more than 200 employees have trained to perform vulnerability assessments, and a growing cadre has passed a rigorous six-hour exam to become Certified Information Systems Security Professionals. FAA is cooperating with other government agencies, such as the National Security Council, the Department of Defense (DOD), and the National Institute of Standards and Technology (NIST), to develop a process for certification and authorization in both new and legacy systems.

In accordance with NIST recommendations, FAA also has established a proactive computer security incident response capability (CSIRC) to protect systems and networks from external and internal denial or disruption (4). The CSIRC seeks to accomplish six goals:

- ◆ Centralize reporting of computer security incidents involving national airspace, mission support, and administrative systems;
- ◆ Provide expert assistance to detect, isolate, contain, and eliminate incidents and malicious code that threaten the integrity, availability, or confidentiality of FAA systems;
- ◆ Coordinate response to computer security incidents;
- ◆ Provide direct technical assistance to secure FAA information systems under the jurisdiction of other entities;
- ◆ Provide an electronic clearinghouse for computer security information; and
- ◆ Provide liaison to law enforcement agencies and criminal investigations.

Aiming at near-term objectives and benefits, the awareness and execution activities rely on disciplined program management, analogous to the skills that made FAA's Y2K program successful. FAA is not only taking advantage of lessons learned from Y2K but also has assigned some of the seasoned Y2K managers to the information systems security program.

Architecture and Engineering

The left face of the pyramid, architecture and engineering, addresses longer-term planning for FAA information systems security. Architecture and engineering requires the effective management of an ongoing research and development program, including the application of new technologies—such as biometrics to reduce reliance on passwords—and dividing security measures optimally among transport, network, and applications systems.

The architecture and engineering endeavors have made early progress with the recent release of the FAA information systems security architecture, which will be updated regularly. The architecture document details security requirements and services and allocates proposed services to the national airspace subsystems that process, communicate, and control sensitive ATC information. In addition to providing a design for integrating security measures into the national airspace system, the architecture offers alternatives for the analysis of capital investments and a phased roadmap for responding to PDD-63.

The security services derive from requirements defined in policy assessments of ATC operations as well as

- ◆ Vulnerability analyses that indicate what and where security services are needed to prevent interference with safe and continuous ATC operations;
- ◆ Threat assessments that emphasize why security is needed, revealing mechanisms capable of exploiting vulnerabilities; and
- ◆ Risk assessments that show how extensively and when security services are needed, examining the impact of combined threats to points of vulnerability in the system.

Several industry advisory groups and other government agencies reviewed the FAA's information systems security architecture. Revisions based on their comments and suggestions were inserted in Version 1.1. FAA expects to provide the next version by the end of FY 2001.

R&D activities will include the development of

- ◆ Intrusion detection technology that produces fewer false positives than current commercial products (l, p. 113),
- ◆ Tools to aid in the design of information systems security architectures,
- ◆ Tools to monitor and overcome agents that attack IT resources,
- ◆ Technologies and procedures for Public Key Infrastructure (l, pp. 124-132), and
- ◆ Tools to defend against denial-of-service attacks (l, pp. 149-150).

The architecture and engineering area involves long-term planning and deliberations, facing more extensive challenges than those of Y2K, which involved a known problem with a known solution and a known date. In contrast, information systems security faces threats in many forms, at many times, ever changing as technology forges ahead. To meet this challenge, FAA is drawing on talents of personnel from DOD and also from systems engineers who have worked on the design of the national airspace system.

The architecture-and-engineering and the awareness-and-execution activities complement each other, providing a world-class, near-term program management process that receives new direction as technology evolves. The goal is to blend these two sides of the pyramid to ensure the strength of all the layers of protection.

Life-Cycle Model

Figure 3 depicts the FAA's life-cycle model for information systems security, applicable to the structural, operational, and process models. The four interconnected steps of the plan, do, check, act model—that is, plan, protect, detect, and respond—repeat as new threats emerge and new technology and procedures are applied.

A security system should protect against known threats, detect attacks, determine the success or failure of the attacks, and respond as necessary. After each attack, the system should initiate procedures to analyze what happened, assess the impact, and revise plans accordingly, designing and installing new and improved protections and keeping protection and response capabilities current and effective.

Meeting the Critical Challenge

Information systems security promises to be one of the most critical challenges facing the United States in the next decade. FAA is establishing plans and programs to meet the challenge.

Although efforts in FY 1999 and FY 2000 faced severe budget constraints, FAA has responded proactively to PDD-63, establishing a base for future initiatives. If the FY 2001 budget reflects the size and scope of the information systems security task, FAA will be able to implement its full information systems security program.

FAA's objective is to expand both the certification and authorization processes as well as the operation of the CSIRC. In addition, FAA intends to revise its information systems security architecture to address the national airspace system and other elements by the end of FY 2001. FAA should meet and even exceed the PDD-63 requirements by the May 2003 deadline and expects to continue information systems security endeavors beyond that.

Acknowledgment

The author thanks members of the executive team of FAA's Office of Information Services who assisted in the preparation of this article.

References

1. *Trust in Cyberspace* (Schneider, F. B. ed.). National Academy Press, Washington, D.C., 1999.
2. *Aviation Security: Vulnerabilities Still Exist in the Aviation Security System*. GAO/T-RCED/AIMD-00-142, Government Accounting Office, Washington, D.C., April 2000, p. 4.
3. Ibrahim, L., et al. *The Federal Aviation Administration Integrated Capability Maturity Model (FAA-iCMM), Version 1.0*, Nov. 1997.
4. Wack, J. P. *Establishing a Computer Security Incident Response Capability (CSIRC)*. NIST SP-800-3, National Institute of Standards and Technology, Gaithersburg, Md., Nov. 1991.