

NAS Information Security (INFOSEC)

With the implementation of open architectures and open communications protocols throughout the National Airspace System (NAS), there is an increased vulnerability to information security attacks.

Technical Center Activities

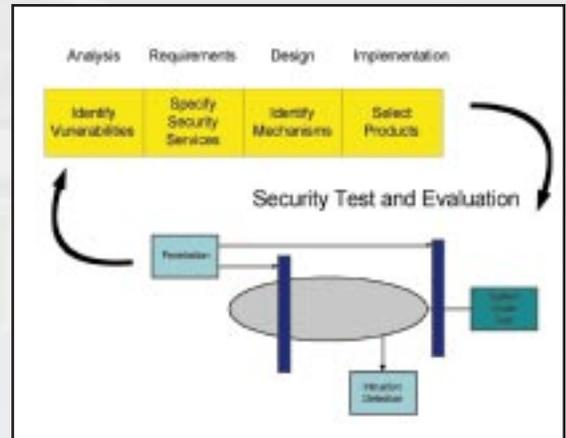
ACT-350 of the Communications/Navigation/Surveillance Engineering and Test Division, under sponsorship from ASD-110, the NAS Architecture Branch of the Office of System Architecture and Investment Analysis, has implemented a Security Test and Evaluation (ST&E) Program. ACT-350 is taking a total life-cycle approach to ST&E as is depicted in the figure to the right.

ACT-350 performs the following activities:

- ST&E Laboratory
- ST&E Program
- Penetration Testing
- Intrusion Detection
- Security Prototyping
- Security Certification Support

ST&E Laboratory

One of the major milestones of 1998 was the establishment of a Security Test and Evaluation Laboratory at the William J. Hughes Technical Center. The ST&E laboratory provides a central facility which can be used by any organization for penetration testing, security test and evaluation, or security product evaluation.



ST&E Program

ACT-350 is developing INFOSEC testing guidance materials as part of the overall ST&E program. Guidance materials will be consistent with the Acquisition Management System (AMS) Test and Evaluation Process Guidelines and will include example INFOSEC Critical Operational Issues (COIs) and associated Measures of Effectiveness, Suitability, and Performance (MOEs, MOSs, and MOPs).

Penetration Testing

The ST&E laboratory was used to conduct penetration of the Host Interface Device/NAS Local Area Network (HID/NAS LAN). This activity demonstrated the vulnerability of NAS subsystems to attack in the absence of appropriate protection mechanisms. The activity did not stop with the system penetration. Rather, subsequent analysis identified fixes which are being applied to secure the HID/NAS LAN.

Efficiency
System



System Efficiency

Intrusion Detection

The ST&E laboratory will be used by the FAA for evaluation of intrusion detection products and systems. There is a recognized need for insertion of intrusion detection systems into NAS subsystems. The ST&E laboratory will be used to determine the suitability of commercial, off-the-shelf systems and to determine unique NAS requirements in this area.

Security Prototyping

The ST&E laboratory will be used for prototyping security services in select NAS subsystems. Prototyping will be performed to determine the general feasibility of adding cryptographic and other security services to these systems. Prototyping will identify resource requirements and potential performance impacts, e.g., computational and protocol overhead. Prototyping will also determine additional measures which must be applied for secure acquisition of keys and for protection of keys in the operating environment and will identify security system management functions, such as security alarm reporting and audit trail.

Security Certification Support

ACT-350 has a staff of experienced security system engineers. ACT-350 support can be provided to other organizations to help, for example, in developing security plans for their specific subsystems.

For additional information, contact:

Communications/Navigation/Surveillance Engineering and Test Division, Data Link Branch

Federal Aviation Administration
William J. Hughes Technical Center
Atlantic City International Airport, NJ 08045
Phone: (609) 485-6304
Fax: (609) 485-6566