Cyber Assurance

Christopher Alberts, Robert J. Ellison, and Carol Woody

Project Description

Cyber assurance is the justified confidence that networked systems are adequately secure to meet operational needs, even in the presence of attacks, failures, accidents, and unexpected events. This requires appropriate consideration of operational security across all aspects of acquisition, development and deployment, and operations and sustainment.

Existing assurance approaches are primarily single system, single organization focused. With the highly interconnected, complex environments in use today, effective cyber assurance must be addressed across multi-program acquisitions, through the supply chains, and among operational environments that span multiple organizations.

In addition, security considerations are typically handled by experts operating outside of the normal acquisition and development workflow addressing certification and accreditation activities. Instead, cyber assurance must be effectively fused with day-to-day acquisition, development, and operational activities and not viewed as separate add-on actions.

In order to assure the operational security characteristics of networked systems, appropriate methods and metrics for managing and monitoring are critical.

Decisions impacting security are made at multiple levels of the organization as well as across the acquisition life cycle, but there is not an effective means of bridging among the range of stakeholders, which can include program management, architects, system and software engineers, implementation support, security specialists, operational management, and operational support. An integrated decision-making framework is needed that can link a management perspective with the detailed technical and operational realities so that the impact of decisions made at each level can be determined and appropriately evaluated. For example, this integrated view would allow cost and schedule options to be evaluated against the operational security risk.

Research tasks will include

- development of assessment techniques for cyber assurance in multi-system, multi-enterprise environments
- establishing an integrated decision-making framework
- building best practices for cyber assurance relative to acquisition, development and deployment, and operations and sustainment
- identification and use of metrics to monitor and manage cyber assurance
- approaches for using modeling and simulation to analyze and improve cyber assurance

References

Ellison, R., Goodenough, J., Weinstock, C., and Woody, C. Survivability Assurance for Systems of Systems, Software Engineering Institute, Carnegie Mellon University, CMU/SEI-2008-TR-008, http://www.sei.cmu.edu/publications/documents/08.reports/08tr008.html

Alberts, C., Smith II, J., and Woody, C. Multi-view Decision Making (MVDM) Workshop, Software Engineering Institute, Carnegie Mellon University, CMU/SEI-2008-SR-035, http://www.sei.cmu.edu/publications/documents/08.reports/08sr035.html

Alberts, C., Woody, C., "Consider Operational Security Risk During System Development" published in IEEE Security & Privacy January/February 2007