Homeland Security

Software Assurance

DHS Cyber Security

Software is essential to the operation of the Nation's critical infrastructure. Software vulnerabilities can jeopardize intellectual property, consumer trust, and business operations and services. In addition, a broad spectrum of critical applications and infrastructure, from process control systems to commercial application products, depends on secure, reliable software.

The Software Engineering Institute estimates that 90 percent of reported security incidents result from exploits against defects in the design or code of software. Ensuring software integrity is key to protecting the infrastructure from threats and vulnerabilities and reducing overall risk to cyber attacks. To ensure system reliability, integrity, and safety, it is critical that provisions be included for built-in security of the enabling software.

Setting a Higher Standard for Software Assurance

Grounded in the National Strategy to Secure Cyberspace, the Department of Homeland Security's (DHS) Software Assurance Program not only spearheads the development of practical guidance and tools but also promotes research and development investment in cyber security. The program provides support and guidance for significant new research on secure software engineering. This research is examining a range of development issues, from new methods that avoid basic programming errors, to enterprise systems that remain secure when portions of the system software are compromised.

Through these efforts, DHS seeks to reduce software vulnerabilities, minimize exploitation, and address ways of improving the routine development and deployment of trustworthy software products. Together, these activities will enable more secure, reliable software that supports mission requirements across enterprises and the critical infrastructure.

From Patch Management to Software Assurance

The key objective of the Software Assurance Program is to shift the security paradigm from patch management to software assurance. This shift is designed to encourage software developers to raise overall software quality and security from the start rather than rely on applying patches to systems after vulnerabilities have been identified.

Recognizing that software security is fundamentally a software engineering issue that must be addressed systematically throughout the software development life cycle, DHS encourages all software developers, as well as the public sector and private industry, to raise the standard on software quality and security. Working together, government, industry, and academia can raise expectations for product assurance with requisite levels of integrity and security by promoting security methodologies and tools as a normal part of business.

Building Success Through Collaboration

Public-private partnerships form the foundation of the Software Assurance Program. By partnering with the private sector, academia, and other federal departments and agencies, the program seeks to influence improvements in software development, quality assurance, and acquisition processes that will lead to producing higher quality, more secure software. Toward this end, DHS is sponsoring conferences and workshops, a common body of knowledge, and a web-based repository of practical guidance for software developers and architects.

In collaboration with industry, academia, and government partners, DHS's approach to addressing software assurance encompasses the following components:

- **People**—Education and training for developers and users
- **Processes**—Practical guidelines and best practices for the development of secure software
- **Technology**—Analysis of tools for evaluating software vulnerabilities and quality
- **Acquisition**—Specifications and guidelines for acquisition and outsourcing.

Obtaining Additional Information

To learn more about DHS's Software Assurance Program, visit us at **https://buildsecurityin.us-cert.gov**

Cyber security is a shared responsibility. Working together, we can secure America's cyberspace.