Engineering Security Into the Software Development Life Cycle

Gary M. McGraw
Cigital Inc.

Nancy R. Mead
Software Engineering Institute

The Build Security In (BSI) initiative seeks to alter the way software is developed so that it is less vulnerable to attack when security is built in from the start. BSI is part of the Software Assurance Program within the Strategic Initiatives Branch of the National Cyber Security Division of the Department of Homeland Security. As part of the initiative, a BSI content catalog is available on the U.S. Computer Emergency Readiness Team Web site. It is intended for use by software developers and software development organizations who want information and practical guidance on how to produce secure and reliable software.

Today's large-scale, highly distributed, networked systems improve the efficiency and effectiveness of organizations by permitting whole new levels of organizational integration. However, such integration is accompanied by elevated risks of intrusion and compromise. Incorporating security and survivability capabilities into an organization's systems can mitigate these risks.

Typical software development life-cycle models do not focus on creating secure systems, and fall short when the goal is to develop systems with a high degree of assurance [1]. If addressed at all, security issues are often relegated to a separate thread of project activity, with the result that security is treated as an add-on property. This isolation of security considerations from primary system-development tasks results in an unfortunate separation of concerns. Security should be integrated and treated on par with other system properties to develop systems with required functionality and performance that can also withstand failures and compromises [2].

The Build Security In Software Assurance Initiative

The Build Security In (BSI) Software Assurance Initiative seeks to alter the way that software is developed so that it is less vulnerable to attack and security is *built* in from the start. BSI is a project of the Strategic Initiatives Branch of the National Cyber Security Division (NCSD) of the Department of Homeland Security (DHS).

Figure 1: *BSI Content Catalog Components*

BEST PRACTICES	KNOWLEDGE
Risk Management	Software Development Life Cycle
Project Management	Business Relevance
Assembly, Integration, and Evolution	Attack Patterns
Architectural Risk Analysis	Principles
Threat Modeling	Guidelines
Measurement Code Analysis	Historical Risks
Security Testing	Coding Practices
Measurement	Coding Rules
Incident Handling and Monitoring	**TOOLS**
Penetration Testing	Modeling Tools
White Box Testing	Code Analysis
Deployment and Operations	Black Box Testing Tools

The initiative includes a BSI content catalog available on the U.S. Computer Emergency Readiness Team Web site at <http://BuildSecurityIn.us-cert.gov>. It is intended for use by software developers and software development organizations who want information and practical guidance on how to produce secure and reliable software. The catalog is based on the principle that software security is fundamentally a software engineering problem and must be addressed in a systematic way throughout the software development life cycle. The catalog either contains or links to a broad range of information about best practices, tools, guidelines, rules, principles, and other knowledge to help organizations build secure, reliable software.

Figure 1 identifies aspects of software assurance that are covered in the catalog and how the material has been organized. It categorizes catalog content according to best practices, knowledge, and tools, and includes business cases.

Best Practices

A significant portion of the BSI effort will be devoted to best practices that can provide the biggest return considering current best thinking, available technology, and industry practice.

Knowledge

Recurring patterns of software defects leading to vulnerabilities have been identified, and the BSI team is documenting detailed instructions on how to produce software without these defects under the headings "Guidelines," "Coding Practices," and "Coding Rules."

Tools

The BSI site includes information about the kinds of tools that can be used by both developers and security analysts to either detect or remove common vulnerabilities.

Business Cases

Business cases help convince industry to adopt secure software development best practices and to educate consumers on the need for software assurance. Each documented best practice addresses the business case for use of that practice. An overall business case framework will be included.

Future Plans

The DHS NCSD has invited representatives from industry, academia, and government to become involved. Part of this outreach activity includes seminars at which invited organizations can receive and share information about software assurance resources and help the stakeholder community understand both the need for building security in and the value of the Web site for providing relevant guidance. Content will be linked with reference sources and other materials made available through the DHS NCSD Software Assurance Program such as information in "security-enhancing the application software development life cycle" and the software assurance common body of knowledge, which provides a framework for education and training curriculum development in software assurance.◆

References

1. Marmor-Squires, A.B., and P.A. Rougeau. Issues in Process Models and Integrated Environments for Trusted Systems Development. Proc. of the 11th National Computer Security Conference. Fort George G. Meade, MD, Oct. 17-20, 1988: 109-113.
2. Mead, N.R., et al. "Managing Software Development for Survivable Systems." Annals of Software Engineering 2 (2001): 45-78.

Point of Contact

Jan Philpot
Software Engineering Institute
4301 Wilson BLVD STE 200
Arlington, VA 22203
Phone: (703) 908-8208
Fax: (703) 908-9317
E-mail: philpot@sei.cmu.edu