CERT | Software Engineering Institute
Carnegie Mellon University

SUPPLY CHAIN AND COTS ASSURANCE

Organizations are increasingly acquiring commercial-off-the-shelf and open source software products or outsourcing development. Current approaches to acquisition do not account for the risk management issues of complex software supply chains. On-time delivery and costs often get attention, but some of the most serious risks are related to system assurance, the confidence that the system behaves as expected. Software defects, such as design and implementation errors, can lead to unexpected behaviors, system failure, or vulnerabilities that can lead to attacks.

Our approach to assure the security of supply chains can help acquirers in several ways.

Assist with applying existing techniques to reduce software supply chain risk. The immediate problem is not the need for new techniques but the application of known effective methods. For example, countermeasures for SQL injections are well established, yet SQL injections still rank second on the MITRE/SANS list of the top 25 most dangerous software errors.

We can help your organization apply the appropriate techniques in these acquisition scenarios:

- commercial products: assess a specific product as well as supplier capabilities to develop secure software
- custom-developed software: as part of selecting a supplier, assess the supplier's ability to evaluate and mitigate supply chain risks associated with product selection and integration and with subcontractor supplier software; also monitor supply chain risks during development
- supply chain integrity: protect components during development and in transit among participants in a supply chain

Provide guidance on managing supply chain risks. The most significant supply chain risks can occur after deployment. Risk assessments done with the initial acquisition are invalidated over time by new threats and attack patterns, product upgrades or replacements, and changes in consequences with expanded usage. Frequently there is a change in contractors from development to sustainment with a potential change in supplier capabilities. We will help your organization understand and identify critical supply chain risks.

Help acquirers most effectively use their resources in considering supply chain risks. We can provide a framework that helps your organization understand the supply chain factors that arise from tradeoffs among business risks, sources of those risks (suppliers, features, and usage), and possible risk mitigations (supplier selection, feature usage, integration, and risk acceptance). For example, retailers, manufacturers, and suppliers that participate in a distributed inventory system can be at risk when one of the other participating systems is compromised.

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu | www.cert.org
Email: info@sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0004411