Thoughts on the Microsoft SDL

by Robert Harvey, Senior Security Consultant

Using a Secure Development Lifecycle (SDL) is an important practice because it produces more secure software from the start and saves money in the long term. SDL is a software development lifecycle with security milestones and processes built into your overall software development methodology. The goal of an SDL is not only to produce more secure software, but to reduce the overall lifetime cost of software development projects due to the need for security bug fixes.

A study published by Kevin SooHoo, Andrew W. Sudbury, & Andrew R. Jaquith in "Tangible ROI through Secure Software Engineering", Secure Business Quarterly, Volume 1, Issue 2, cited statistics originally developed by the IBM Systems Sciences Institute statistics. This study demonstrates the relative cost of addressing security issues throughout a Software Development Lifecycle.

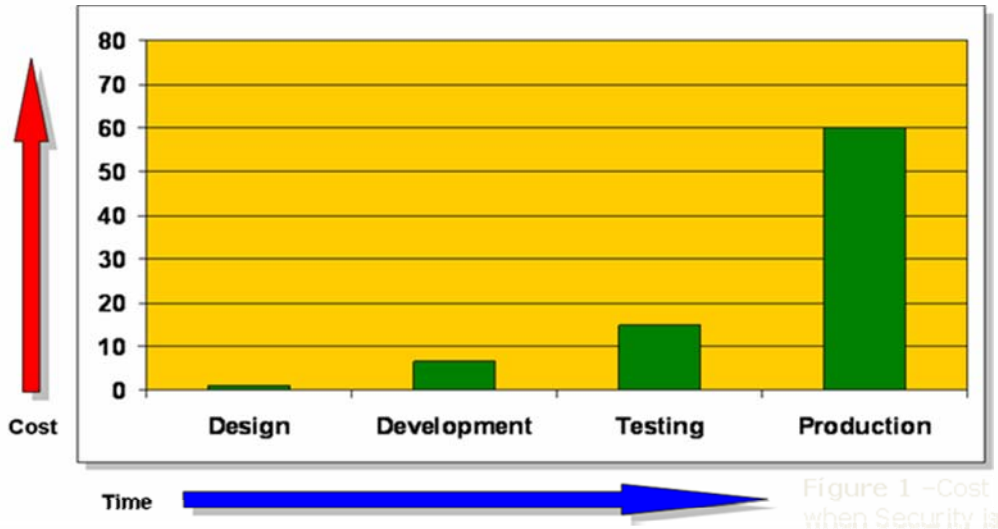

Figure 1 –Cost Multipliers when Security is Applied Late in an SDLC[1]

[1] IBM System sSciences Institute statistics, cited by Kevin SooHoo, Andrew W. Sudbury, and Andrew R Jaquith in "Tangible ROI through Secure Software Engineering Secure Business Quarterly, Volume 1, Issue 2.

The most common SDL was pioneered by Microsoft over the past few years, starting when Bill Gates wrote his famous "Trustworthy Computing" memo[1]. Microsoft's Vista was the first major software release done entirely within that SDL. The Windows Vista Year One Vulnerability Report[2] demonstrates that significantly fewer patches had to be released for Windows Vista in its first full year of release, as compared to Windows XP. Specifically, in its first full year of release Windows Vista had 17 security updates issued, addressing a

[1] <http://www.microsoft.com/mscorp/execmail/2002/07-18twc.mspx>

[2] <http://www.microsoft.com/windowsserver/compare/ReportsDetails.mspx?recid=54>

total of 36 security vulnerabilities. By comparison, Windows XP—released prior to the inception of SDL—had 30 security updates issued in its first full year addressing a total of 65 security vulnerabilities.

While the Microsoft SDL may not be a perfect fit for every organization, it is one of the best-known and most mature examples. I recommend that organizations who do not yet have an SDL start with the Microsoft model and customize it to fit their company's needs.

Further Reading

Microsoft SDL Blog—<http://blogs.msdn.com/sdl/default.aspx>

Blog of Jeff Jones, Strategy Director, Microsoft Security Technology Unit—<http://blogs.technet.com/security>

US Department of Homeland Security National Cyber Security Division, “Estimating Benefits from Investing in Secure Software Development”—<https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/business/267-BSI.html>

About Robert Harvey

Robert Harvey is a privacy expert who has been involved in more than 1000 penetration tests and written hundreds of threat models. As a senior security consultant at IOActive, he performs security review and penetration testing for clients in a variety of industries, including software development, financial services, healthcare, high-tech, education, government, and other mid-size and Fortune 500 companies. Mr. Harvey has extensive experience in risk management and is at work developing a tool to more easily communicate the results of threat modeling, as well as a methodology to improve and expand the building of threat models in general. He also has helped many clients achieve compliance with regulations such as SOX and HIPAA.