

It's Time to Provide Security Requirements to Software Providers!

It is time for each of us to reconsider our requirements for software and include security in our core requirements. This applies on a corporate, organizational and personal level. So why now? We created a universal demand for software functionality in almost every product and service provided by commercial and non-profit enterprises on a global basis. The software industry has responded well to our requirements to date and has focused on delivering enabling functionality to meet our time to market requirements. If we don't change our requirements, we shouldn't expect software providers to change how they deliver functionality to us.

Software vendors give us what we want but not what we need

Unfortunately, we have never really specified that we prefer software to be free from security vulnerabilities, nor have our buying habits indicated that this is crucial to our success. The large majority of software Requests For Proposals (RFPs) do not specify the identification of controls in the software development process to identify and remediate security flaws. In fact, "researchers" not actual consumers identify most security vulnerabilities. Software vendors have responded by consistently releasing software patches that address known vulnerabilities as quickly as they can. To blame software vendors for the growing level of security vulnerabilities in commercial software products today is not all that effective at yielding better results and is somewhat off the mark. Software vendors have largely given us what we have asked for, functionality rapidly delivered on open standards based platforms. Their business models reflect the churn for new functionality delivered rapidly to the market and those that have mastered this process meet both consumer and Wall Street expectations. Consumers created the demand for the current model and consumers are going to have to change it to expect different results from software vendors.

Software drives the world's infrastructure

It is time for us to change requirements and our expectations. Software, whether commercially produced or organically developed by IT organizations, has become core to the infrastructure of the global economy. Very few products and/or services can be provided effectively or distributed effectively today without the functional contribution of software. Every time you travel by air today, the planes you fly in were designed, manufactured, operated and maintained by processes solely dependent on software functionality. The food we eat, the cars we buy, and goods we acquire at auction on e-bay are all enabled by software. Yet with all of this demand for functionality from software, there remains limited understanding of how to assess an effective process for creating resilient software with limited security vulnerabilities that can be exploited via the Web.

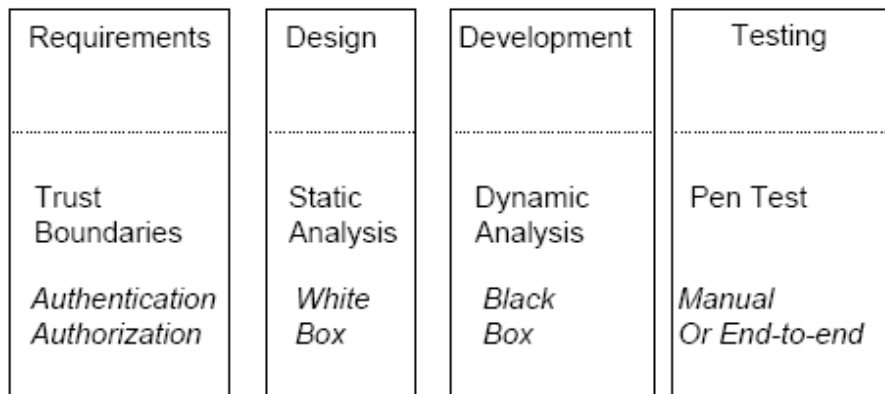
It is time for the buyers of software to fundamentally change requirements whether we are buying a new enterprise wide ERP solution for a growing business or buying *The Sims 2* for our children's home PC. This includes software development that we outsource offshore as well as software we build internally.

The Best Software Developers Create Code with Vulnerabilities

Designing software that is functional and works consistently is a challenging endeavor in the best of circumstances and most software developers understand that there is really no way to guarantee quality in software design and development regardless of the level of talent. The best software developers create great functionality that can be hacked due to vulnerabilities in the code. Software developers are typically very good at creating functional code. However, the skill necessary to “break” an application the way a hacker would is unique and very difficult to teach to a software developer. The tools and services available to detect vulnerabilities early in the software development lifecycle and correct them before the cost of remediation increases significantly are improving daily. There is clearly a large body of evidence to suggest that using a consistent, repeatable process followed by established practices does improve the probability of success. The same is true for designing and building software with limited security vulnerabilities and consumers or business users can and should require the adoption of good practices to eliminate software defects related to security within the software development lifecycle.

A Good Enough Practice Today

Here is a simple model that commercial consumers, business users, and PC users should consider before buying commercial software or hiring an internal or external organization to build software.



There are four boxes representing the core phases of most software development lifecycle methodologies. The terms on the lower part of the boxes are the security related deliverables or activities that represent current industry practices for improving software security. The terminology may vary but as a buyer of a software product or outsource development project, I should ask vendors to demonstrate to me that they incorporate these practices into their software development process. There are many different ways for vendors to demonstrate compliance with this model. Many products and tools are available today that can be highly effective in determining vulnerabilities during the development cycle allowing developers to correct them prior to coming to market with their software.

It is time for the software buyers or acquirers to change requirements to include a demonstration of compliance with evolving practices to improve software security. This can do more to improve software security than any other single action and if we start today, perhaps we can avoid a catastrophic loss attributed to infrastructure dependent software with security vulnerabilities that are exploited due to weak security controls in the software development process.

Jim Routh is the CISO for The Depository Trust & Clearing Corporation (DTCC). This paper represents his views and not necessarily the views of DTCC.

The Depository Trust & Clearing Corporation (DTCC), through its subsidiaries, provides clearance, settlement and information services for equities, corporate and municipal bonds, government and mortgage-backed securities and over-the-counter derivatives. In addition, DTCC is a leading processor of mutual funds and insurance transactions, linking funds and carriers with their distribution networks. DTCC's depository provides custody and asset servicing for 3.5 million securities issues from the United States and 100 other countries and territories, valued at \$40 trillion. In 2007, DTCC settled more than \$1.8 quadrillion in securities transactions. DTCC has operating facilities in multiple locations in the United States and overseas.