How do we ensure that software actually works the way it is designed to work?

We use software quality assurance (SQA), which I began doing as part of my job as a member of a compiler-writing team in 1979. It became evident very quickly that manual methods of SQA are a hopelessly inefficient and ineffective way of finding errors in software. We absolutely have to implement automated testing to have any hope of catching errors in the software we write (or test).

Recently I had the privilege of interviewing Andy Chou, Chief Scientist & Co-founder of Coverity. Here is the first of three parts of our edited conversation about automated software quality assurance (ASQA).

1) Tell the readers about your experience in SQA.

My experience with software quality assurance, or software integrity, began when I was a PhD student at Stanford doing research on static analysis. My colleagues and I quickly realized that companies didn’t have access to analysis technologies that could scale to their large, complex code bases. Lives and businesses rely on software staying functional every day, yet there were no commercial software integrity solutions available. We recognized this need as we were developing the technology and were able to bring Coverity to market.

Since founding Coverity, we’ve helped numerous major enterprises and government organizations improve their products and technologies by implementing automated source code static analysis. We’ve also worked with the open-source community to ensure that static analysis technologies are applied to open-source systems to harden the infrastructure of those projects.

A large part of our job is working with software development organizations to get their developers to adopt static analysis and other software integrity solutions. For a developer, it represents a change to how they work and it changes what they expect from their development tools. It can be a challenge.

2) When and how did you get involved with automated ASQA?

We initially brought Coverity to market because we believed the commercial application of this technology was nowhere near its potential. The research and academic communities were missing something. We knew we had an important problem to solve.

Traditional software integrity testing had fundamental problems. At the time, testing was more
about monitoring for failure than preventing defects. You were relying primarily on testing by
developers, and individual developers are only as good as their best effort – they’re human,
they’re fallible, they can miss things. Getting coverage of all of the possible behaviors was very
difficult with traditional testing. There are enormously many execution paths in code of even
moderate size, and even exceptionally well-tested systems had limited test coverage. And testing
was expensive.

The inadequacy of manual testing became distinctly apparent as we were conducting research for
a paper we planned to publish; as part of our research, we ran automated static analysis on the
Linux kernel. In just one weekend, with little effort, we found hundreds of defects in the code.
We found so many bugs, so quickly! It really was an “aha” moment for us – we realized that
with this technology we could fundamentally change how software is developed.

More of this interview in the next two columns.

* * *

Andy Chou<http://coverity.com/html/about_leadership.html>, PhD is co-founder and Chief
Scientist of Coverity, Inc.<http://coverity.com/html/about_fact.html> He is responsible for
advancing source code analysis technology at Coverity as well as furthering the state of the art in
software integrity industry-wide.

M. E. Kabay,<mailto:mekabay@gmail.com> PhD, CISSP-ISSMP, specializes in security and
operations management consulting services and teaching. He is Chief Technical Officer of
Adaptive Cyber Security Instruments, Inc.<http://acsi-cybersa.com/> and Associate Professor
of Information Assurance<http://norwich.edu/academics/business/infoAssurance/index.html>
in the School of Business and Management<http://norwich.edu/academics/business/faculty.html>
> at Norwich University.<http://www.norwich.edu> Visit his Website for white papers and

Copyright © 2010 Andy Chou & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without
limit on any Web site, and to republish it in any way they see fit.