Managing a software project—the dos and don’ts

SI2 PI Meeting
January 18, 2012

Von Welch
Director and PI
CTSC
Center for Trustworthy Scientific Cyberinfrastructure (CTSC)

Jim Basney, Randal Butler, Scott Koranda, Jim Marsteller, Bart Miller, Von Welch

We don’t make the software, we help make it more secure (so you can focus on what you do best).

Lots of software development (MyProxy, CILogon, GridShib, COmanage), testing (FPVA), and operating (XSEDE, OSG, LIGO, NCSA, PSC) experience.
CTSC trustedci.org

We engage with projects, and develop training to solve security challenges and we want to help your project.

Let us know your needs: trustedci.org/sw-survey/

Or
Email me (vwelch@indiana.edu)
To Phil’s charge...

What are the security do’s and don’t for vulnerability handling for release, support and testing?

Considering software of maturity to be used in production science project or facility such as OSG, XSEDE, LIGO, IU, NCSA, etc.

This is in a range of maturity, which is separate discussion.
Vulnerabilities

Like the common cold, we’d love to eliminate vulnerabilities, but today everybody gets them.

It’s how you handle them that is important to people trusting your software.

A timely, predictable process is the key.
Support

Do know what versions you support, be clear about that.

Do have a clear process for reporting vulnerabilities.
   E.g. http://grid.ncsa.illinois.edu/myproxy/security/#vh

Do have a internal process for handling vulnerabilities.
   Who is in charge, sets priority, etc.

Do know what software you depend on and monitor them for vulnerabilities – you own those as well for your users.
Release

Do produce a clean fix.
I.e. a new release with just the security fix and nothing else.
User want a quick, painless installation, testing as little as possible.

Do plan your communications
Don’t surprise your user community with a security fix.
A private channel to key users is good.
A dedicated, low-volume channel for announcing is good.
Testing

Do test security releases.
Ability to quickly test is key to quick security releases.
Automated testing helpful, e.g. B&T

Software assurance (testing code security) from the start is good.
The earlier, the easier.
Automated help coming in 2014, SWAMP (http://www.cosalab.org/)
Thank you

Von Welch
vwelch@indiana.edu

www.trustedci.org
blog.trustedci.org
twitter.com/TrustedCI

We thank the National Science Foundation (grant 1234408) for supporting our work. The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.