***Open Source and Cybersecurity*: Does open source software have inherent security advantages/disadvantages? What is the evidence?**

Team Members:

Russell Clarke
David Dorwin
Rob Nash

Description:

Our report will contain a discussion of how open source software compares to commercial (closed-source) software with regard to security. Topics will include: Does the open source community find and fix security bugs faster than commercial software? Do corporations use their greater resources to identify more security bugs than a volunteer community? Do corporations have proprietary tools to help them? Can large corporations leverage their size and broad range of applications; can they amortize the cost of tools? Do industry-supported organizations or companies that sell open-source software provide equivalent assistance? How effective are the commercial, public domain, and open source tools? How do they compare historically? How do the deployment mechanisms, distribution paths, and concerns affect the speed with which such bugs are fixed? Do users (administrators or end-users) deploy fixes for one more quickly than the others? Does the source code being available impact the urgency for a fix? Does open source software have inherently less security bugs, as there are “more eyes” on the project, or is open source more vulnerable (because source is available to bad guys)? Does running software on an open-source or closed-source platform have any advantages or disadvantages? What kinds of bugs are found and might exist in both commercial and open source software? Do the two types of software contain different kinds of security bugs, what can we learn from that, and why do these differences exist? We will include examples of bugs, i.e. buffer overflow, granting access privileges, SQL injection, etc. We will also look at how we can improve security for both open source and closed source applications. In addition, we will attempt to separate design issues, such as kernel architecture, and installation base size, from open/closed source issues.

How we intend to divide the work:

We plan to divide up the work evenly between all three members, since we are all UW PMP students and have similar experiences. We will start by having each person do initial research and locate sources. We'll then meet to brainstorm each section, divide up the sections among the team members and do any related research. We'll share resources and notes that we think may be useful for other sections. As we start developing our sections, we'll share our progress with each other. At first, we may have independent documents, but as we make more progress we'll merge them into a single document. We may use LaTeX which would make it easy to manage, share, and merge our documents.