Open and Shut? An Analysis of Vulnerability Discovery Models for Open Source and Proprietary Software

Kemal Altinkemer, Fariborz Farahmand, Jackie Rees, and Chen Zhang
Krannert Graduate School of Management and the Center for Education and Research in Information Assurance and Security (CERIAS)

Introduction

- Need to assess relative security of computing infrastructural components
  - Measures include number of known vulnerabilities
- Do open source software development processes (OSS) lead to fewer reported vulnerabilities in software? (Raymond, 2000)
- Vulnerability discovery models as way to explore this issue

Background

- OSS development compared to proprietary software development
  - OSS developers often, but not always, volunteer effort
  - Motivated by other factors than immediate financial compensation
    - Personal satisfaction/utility
    - Opportunity to learn new skills
    - Future job opportunities
  - OSS source code is freely available for inspection & alteration
  - Proprietary vulnerabilities can only be found through use or inspection
  - OSS vulnerabilities can be found through use or inspection
  - Proprietary vulnerabilities only found through use
  - Essential process of developing software is same

Background

- OSS and proprietary software should have equivalent security, all other things held equal (Anderson, 2005)
- Factors contributing to the practical difference between number of vulnerabilities in OSS and proprietary development
  - Time to market pressures
  - Transaction costs
  - Complexity

Background

- Previous empirical studies on differences between OSS and proprietary vulnerabilities mixed.
  - (Altinkemer, Rees, and Sridhar, 2005; Walia, Rajagopalan, and Jain, 2006)
- Use vulnerability discovery models to see if significant differences exist between the two development paradigms.

Background

- Software defects examined in software reliability literature (Review in Shantikumar, 1983)
- Vulnerability discovery models as a specific class of software reliability models.
- Time based models:
  - Anderson Thermodynamic Model (2002)
  - Rescorla (2005)
  - Musa-Okomoto (1984)

Model

- AML:
  - Typical adoption curve with few early adopters, then a dramatic vertical rise with increase in users, then flattens back out with saturation.
  - Alhazmi and Malaiya (2005) tested AML against other four models on Windows 95, Windows XP, and Red Hat Linux 6.2 and found AML performed better than the other models.

Model

- Data
  - Collected vulnerability data on operating systems from 1989 through December 2005.
  - Data classified by operating system, vendor, and source type (open or closed).
  - Total of 4574 reported vulnerabilities
  - Dropped operating systems with less than 35 reported vulnerabilities
Data

- Final sample held 34 operating systems
  - 15 proprietary and 19 open source
  - Range of 39 to 300 reported vulnerabilities per system
  - 416 reported vulnerabilities (2263 proprietary and 1853 from open source)
  - Discovery date of when vulnerability published in database
- All five models examined. AT excluded from analysis due to lack of fit using χ² goodness of fit test and the Akaike Information Criteria (AIC)
- Several OS had no significant fit on any model
- Other models significant on fewer OS (except AT)
- Systems with significant model fit tended to have higher numbers of cumulative vulnerabilities generally do not fit tested models as well as systems with fewer vulnerabilities
- For those OS's with significant AML model fit, we examined A, B, and C parameter.
  - The A parameter significantly higher for open source compared to proprietary (0.00473 vs. 0.00086) at p<0.046
  - Interpretation: Open source developers discover vulnerabilities much more quickly than proprietary developers
- The B parameter lower for open source than proprietary (94.602 vs. 118.875) but not statistically significant
  - Interpretation: Slightly fewer numbers of vulnerabilities reported for open source than proprietary
- The C parameter is larger for open source than proprietary (1.351 vs. 0.970) but not statistically significant
  - Interpretation: Difficult to make a direct comparison between various operating systems

Results

- Departure from Alhazmi and Malaiya (2005)
  - Likely due to sheer numbers of systems tested.
- AML was best fit in 7 out of 15 proprietary and 10 out of 19 open source OS
- Other models significant on fewer OS (except AT)
- Several OS had no significant fit on any model
- T-tests indicated that systems that fitting one or more models were newer in terms of months since initial release than systems that did not have significant fit
- Systems with significant model fit tended to have fewer vulnerabilities

Discussion

- Further examination indicates that no model adequately fit many operating systems in the sample

Conclusion

- Important differences in vulnerability discovery curves for different sources of operating systems
- Open vs. closed debate still ongoing
- Older systems generally do not fit tested models as well as newer systems
- Systems with higher numbers of cumulative vulnerabilities generally do not fit tested models as well as systems with fewer vulnerabilities
- All have implications for managers allocating resources