CERIAS

the center for education and research in information assurance and security

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
    - 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:
  - Alhazmi-Malaiya Logistic (AML) Model (2005)
  - Anderson Thermodynamic Model (2002)
  - Rescorla (2005)
  - Musa-Okomoto (1984)

Model

Model	Specification	Comment
Anderson Thermodynamic model (AT)	$\Omega(t)=\frac{k}{\gamma}\ln(Ct)$	k is constant, γ used to indicate a lower number of vulnerabilities as time goes by and C is constant introduced by integration.
Alhazmi-Malaiya Logistic model (AML)	$\Omega(t)=\frac{B}{BCe^{-ABt}+1}$	A and B determined empirically by the data and C is constant. B represents the total number of vulnerabilities present in the software.
Rescorla Linear model (RL)	$\Omega(t)=\frac{Bt^2}{2}+Kt$	B and K are regression coefficients of the linear model that fits vulnerabilities with time, and is integrated to derive the cumulative vulnerability model.
Rescorla Exponential model (RE)	$\Omega(t)=N\left(1-e^{-\lambda t}\right)$	N is total number of vulnerabilities in system and λ is rate constant.
Logarithmic Poisson model (LP)	$\Omega(t)=\beta_0\ln(1+\beta_1 t)$	β_0 and β_1 are regression coefficients.

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.
- Do these results hold across all operating systems with reported vulnerabilities? Are there differences in parameters among the various systems?

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

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center

CERIAS

the center for education and research in information assurance and security

Data

- Final sample held 34 operating systems
  - 15 proprietary and 19 open source
  - Range of 39 to 300 reported vulnerabilities per system
  - 4116 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 χ^2 goodness of fit test and the Akaike Information Criteria (AIC)

Data

Operating System	Source Code	AIC Score				Chi-Square Statistic			
		AML	RL	RE	LP	AML	RL	RE	LP
AIX	C	603	726	540	572	215.33	345.58	1822.06	1102.48
BSD/OS	C	1396	1491	1855	1721	149.77	455.30	1174.28	42.59
HP-UX	C	1798	1746	2231	2141	201.46	195.66*	1836.54	979.73
IRIX	C	707	835	928	914	339.22	538.59	3250.12	2264.48
Mac OS X	C	275	279	363	363	91.08*	677.10	1982.40	1685.22
Mac OS X Server	C	795	744	754	755	19.90*	39.92*	265.46	265.84
OpenServer	C	1468	1364	1781	1676	37.46*	24.97*	24.89*	24.91*
Solaris	C	1191	1252	1310	1310	223.16	229.52	2559.71	1487.43
SunOS	C	1000	1029	1310	1242	75.66*	62.90*	111.06*	110.73*
Windows 2000	C	612	838	768	778	88.22*	435.01	1647.65	1007.70
Windows 95	C	617	592	575	752	17.63*	102.26*	75.49*	78.51*
Windows 98	C	362	350	378	378	79.02*	38.29*	24.77*	324.37
Windows ME	C	1322	1421	1458	1459	23.10*	28.61*	34.91*	34.86*
Windows NT	C	577	594	760	737	277.83	523.33	1027.70	1037.23
Windows XP	C	473	489	485	482	101.27	144.39	1009.41	760.88

A lower AIC score indicates better model fit. A higher P-value for χ^2 test indicates a better fit.
Significance Level: * 0.1

Data

Operating System	Source Code	AIC Score				Chi-Square Statistic			
		AML	RL	RE	LP	AML	RL	RE	LP
Conectiva Linux	O	1278	1256	1460	1393	96.53	164.64	117.25	99.66
Debian Linux	O	952	1057	1109	1113	207.49	328.45	1428.66	1001.61
FreeBSD	O	245	281	315	315	72.19*	93.33*	152.16*	156.01
Gentoo Linux	O	1359	1370	1511	1488	59.35	203.64	500.24	499.92
Linux kernel	O	1225	1257	1431	1100	437.02	412.41	2040.89	1619.01
Mandrake Linux	O	780	827	819	819	314.81	640.03	1781.47	1474.45
NetBSD	O	792	708	905	905	55.23*	38.06*	52.51*	52.64*
OpenBSD	O	117	119	142	142	50.37*	24.59*	150.19	150.55
Red Hat Advanced Workstation for the Itanium Processor	O	235	245	267	267	94.98	27.17*	76.78	76.61
Red Hat Enterprise Linux	O	153	169	191	191	71.64	104.55	212.61	212.50
Red Hat Enterprise Linux AS	O	128	146	169	169	15.21*	28.24*	84.34	84.14
Red Hat Enterprise Linux ES	O	151	167	189	189	8.57*	13.47*	45.03	44.80
Red Hat Enterprise Linux WS	O	63	64	70	70	14.23*	26.47*	80.23	79.86
Red Hat Fedora	O	1039	1367	1538	1460	16.18*	16.95*	29.23	28.89
Red Hat Linux	O	71	77	79	78	61.10*	436.18	2451.28	1589.16
Secure Enterprise Linux	O	397	403	419	419	155.71	10.36*	14.48*	13.90*
Secure Linux	O	853	756	749	746	145.37	195.89	252.31	281.87
Slackware Linux	O	67	82	81	81	72.46*	38.98*	38.85*	39.09*
Ubuntu Linux	O	603	726	540	572	9.13*	33.60	36.27	35.83

A lower AIC score indicates better model fit. A higher P-value for χ^2 test indicates a better fit.
Significance Level: * 0.1

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

Results

- 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

Results

- 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

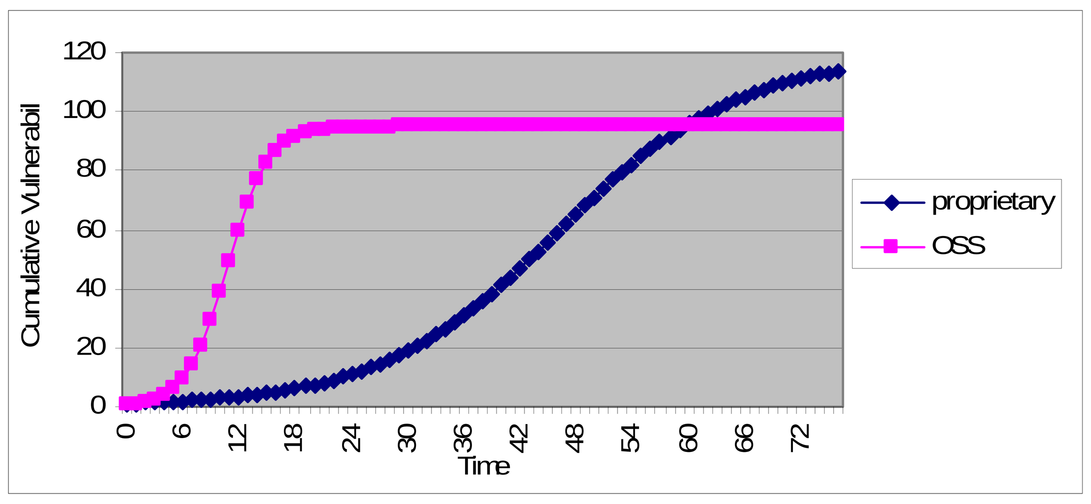

Figure 1: AML model average curves for Proprietary and OSS operating systems

Discussion

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

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

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center