CERIAS

Open Source vs. Proprietary Software: Vulnerabilities and Patch Response

Sanjay Sridhar, Kemal Altinkemer, and Jackie Rees

Overview

- Introduction
- Hypotheses
- Data
- Preliminary Results
- Conclusions and Future Research

Introduction

- Software (S/W) vulnerabilities represent targets for misuse or error
- Software vulnerabilities as software reliability issue
- Patches are released as “solution” to vulnerability
- New S/W releases incorporate previous patches
- Are there differences between patching activities of open source SW developers and proprietary SW developers?

Software Vulnerabilities

- Vulnerabilities can be classified according to:
  - Criticality or Severity level (high, medium or low)
  - Exploit Range (remote or local)
  - Type of Threat
    - Confidentiality
    - Integrity
    - Availability
    - Security Protection

Research Questions

- Are open source developers quicker to release patches than proprietary S/W developers?
- Does open source S/W have fewer vulnerabilities than proprietary S/W?
- Does open source S/W have more severe vulnerabilities than proprietary S/W?
- Are “confidentiality-threat” vulnerabilities more common in open source than proprietary S/W?

Hypotheses - I

- ***Hypothesis 1****: Open source software developers issue patches faster than proprietary software vendors.*
- ***Hypothesis 2****: In unit time, there are fewer vulnerabilities in open source software compared to proprietary software.*
- ***Hypothesis 3:*** *Open source software patches high-severity vulnerability faster than proprietary software.*

Hypothesis - II

- ***Hypothesis 4a:*** *Open source software developers patch confidentiality-type vulnerabilities faster than proprietary software developers.*
- ***Hypothesis 4b:*** *Open source software developers patch integrity-type vulnerabilities faster than proprietary software developers.*
- ***Hypothesis 4c:*** *Open source software developers patch availability-type vulnerabilities faster than proprietary software developers.*
- ***Hypothesis 4d:*** *Open source software developers patch security protection-type vulnerabilities faster than proprietary software developers.*

Data & Methodology

- Operating System Vulnerability and Patch data from the Common Vulnerabilities and Exposures Database (http://www.cve.mitre.org)
- Data collected includes:
  - Vulnerability description
  - CVE key code
  - Date of discovery
  - Date of patch response

Year	Open Source Software			Proprietary Software			T-stat/p-value for difference of Means
	N	Mean (days)	Std. Dev.	N	Mean (days)	Std. Dev.	
2000	37	57.76	57.52	17	35.19	23.00	2.06(0.03)
2001	94	30.64	41.77	83	37.59	47.96	-1.02(0.16)
2002	81	34.12	37.78	105	42.56	47.49	**-1.35(0.09)**
2003	77	29.68	48.26	84	41.12	54.99	**-1.41(0.08)**
2004	16	24.73	14.75	27	24.41	18.50	0.06(0.48)
All	305	34.30	43.81	317	38.90	47.08	**-1.26(0.10)**

Table 1. Mean time to patch for open-source & proprietary operating system software. 1-tailed p-values at the 10% significance shown in bold.

- ❑Open source software has lesser patch-time.
- ❑H1 is partially supported.

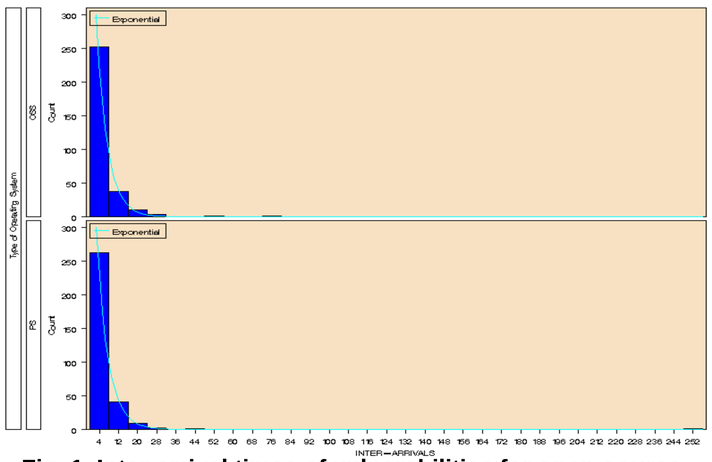

Fig. 1. Inter-arrival times of vulnerabilities for open-source & proprietary operating system software.

CERIAS

Open Source vs. Proprietary Software: Vulnerabilities and Patch Response

Sanjay Sridhar, Kemal Altinkemer, and Jackie Rees

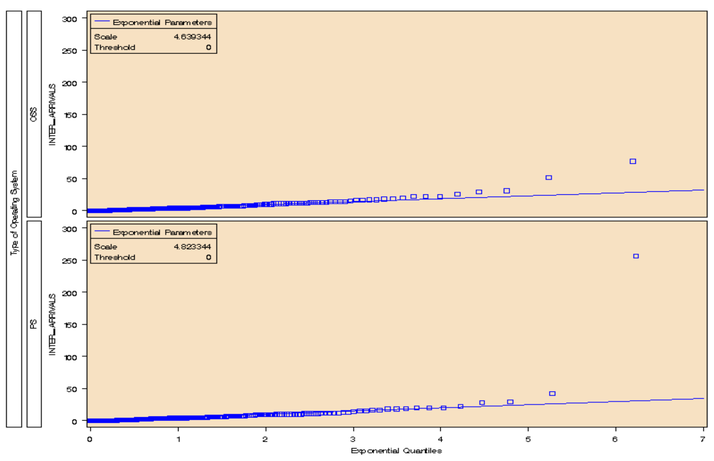

Fig 2. shows the fit of the exponential distribution for inter-arrival times of vulnerabilities.a

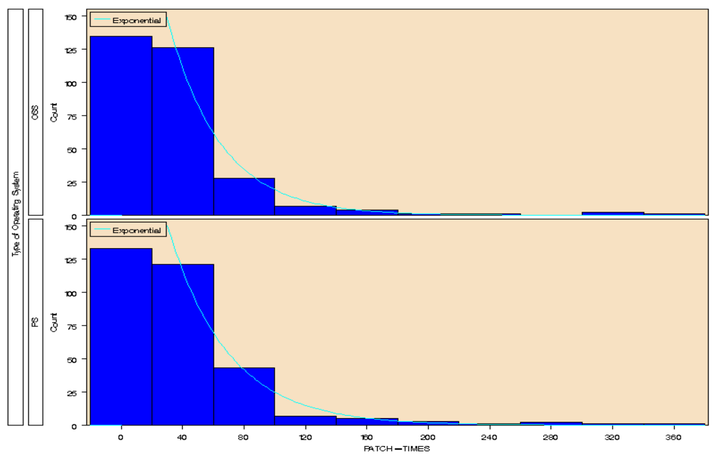

Fig. 3. Overall mean time to patch for open-source & proprietary operating system software.

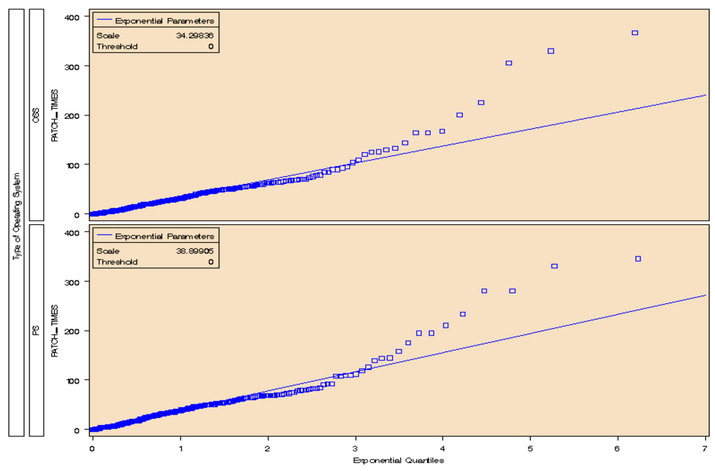

Fig. 4. Fit of the exponential distribution for vulnerability patch-times.

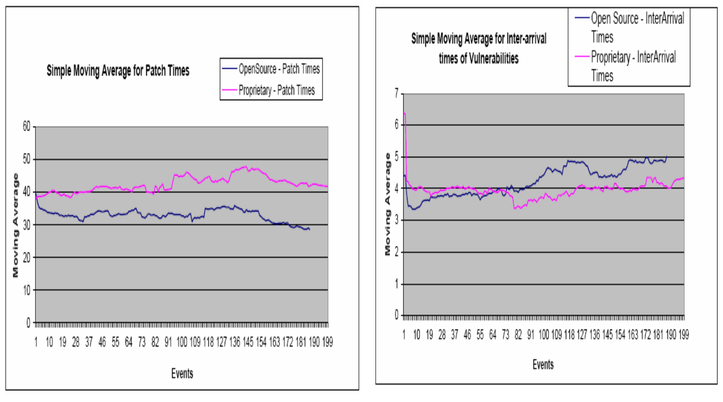

Fig. 5. Simple Moving Average for patch-times and vulnerability inter-arrival times for 120-events interval.

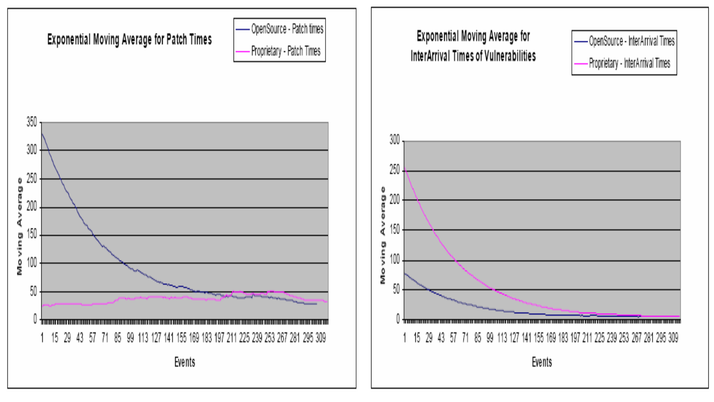

Fig. 6. Exponential Moving Average for patch-times and vulnerability inter-arrival times for 120-events interval.

Type of OS affected	Inter-arrival times of vulnerabilities (T-stat of Difference of means = -0.20)		
	N	Mean (days)	Std. Deviation
O	305	4.64	7.14
P	317	4.82	15.08

Table 2. Mean inter-arrival times of vulnerabilities for open-source & proprietary operating system software.

- ❑ No significant difference between inter-arrival times of vulnerabilities
- ❑ H2 is not supported

Type of Severity	Open Source Software			Proprietary Software			T-stat/p-value for difference of means
	N	Mean (Days)	Std. Deviation	N	Mean (Days)	Std. Deviation	
High	148	34.30	51.30	171	41.99	51.98	**-1.33(0.09)**
Medium	146	33.64	39.53	131	36.11	41.90	-0.50(0.31)
Low	11	42.91	27.64	15	28.07	31.51	1.27(0.12)

Table 3. Severity of the vulnerability. The 1-tailed p-values at the 10% significance are shown in bold.

- ❑ Significant difference in performance regarding high-severity vulnerabilities
- ❑ H3 is supported

Type of Vulnerability	Open Source Software			Proprietary Software			T-stat/p-value for difference of means
	N	Mean (Days)	Std. Dev.	N	Mean (Days)	Std. Dev.	
Confidentiality	41	46.80	38.79	36	35.99	25.44	1.46(0.07)
Integrity	58	32.83	22.24	42	30.46	27.26	0.46(0.32)
Availability	85	45.23	37.06	87	45.43	38.04	-0.04(0.49)
Security Protection	182	47.72	28.75	211	50.38	39.80	0.77(0.22)

Table 4. Type of vulnerability. The 1-tailed p-values at the 10% significance are shown in bold.

- ❑ No significant difference among types of vulnerabilities
- ❑ H4a, H4b, H4c, and H4d not supported

Conclusion & Future Research

- Open-source software appear to be more reliable.
- Develop a software-reliability model.
- Other parameters to evaluate performance (E.g. Number of programmers, maturity of the application)

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center