

“Open Source Software - A Recipe for Vulnerable Software, or The Only Way to Keep the Bugs and the Bad Guys Out?”

Panel at ISSRE 2003

Organizers

Saurabh Bagchi
Dependable Computing Systems Lab
School of Electrical & Computer Engg.
Purdue University, Indiana

Henrique Madeira
Departamento de Engenharia
Informática
Univ. of Coimbra, Portugal

Participants

Andrew Lockhart, IBM Corp. Sean Reifschneider, Tummy.com
Brendan Murphy, Microsoft Corp. Charles Weinstock, CMU

Format

| Item | Max time per panelist (mins) | Max total time (mins) |
|---|-------------------------------------|------------------------------|
| Introductions | 2 | 10 |
| Opening remark by organizers | — | 3 |
| Opening statements by panelists | | |
| Response to pre-proposed set of questions | 5 | 20 |
| Open Q&A from audience | — | 35 |
| Collection of audience poll | — | 2 |
| Closing statements by panelists | 2 | 10 |
| Announcement of poll results | — | 5 |
| Wrap-up | — | 5 |

Pre-Proposed Set of Questions

- What in your mind has been a spectacular success or failure story for open source software?
- How would you define open source software?
- Is open source software without open source hardware useful?
- What software that you use would you most want to be open source?
- Lots of eyeballs means more secure code. Do you agree?
- What are individually likely, feasible, and desirable geographical spread of an open source project?
- Does ethnic or cultural diversity affect an open source project?

Audience Poll Questions

1. Have you used OSS for your product/prototype development?
 - I. No, it leads to sub-standard products
 - II. No, because of legal issues
 - III. Yes, I use it almost solely
 - IV. Yes, I use it somewhat
2. Have you contributed to the OSS movement as a developer?
 - I. No, I have better uses for my time
 - II. No, because of company legal issues
 - III. No, it's on my ToDo list
 - IV. Yes, I have
3. Do you think OSS based products are more reliable to natural failures?
 - I. No
 - II. Yes
 - III. Maybe
 - IV. It doesn't matter
4. Do you think OSS products are more hacker-proof than proprietary software?
 - I. No
 - II. Yes
 - III. Maybe
 - IV. It doesn't matter
5. Which sector do you belong to?
 - I. Academia
 - II. Industry
 - III. Government

Q&A Summary

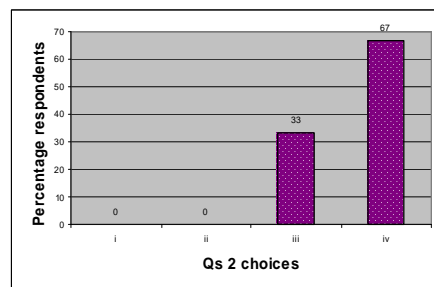
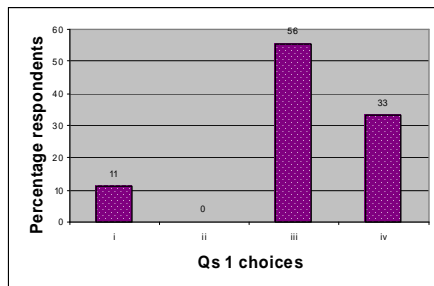
- Here are the questions that were posed by the audience and a digest of the responses from the panelists.
1. Does the fact that industries are now paying employees to develop OSS affect things?
 - “This is likely a passing phase and there will always be a hugely more number of OSS developers who are not paid for their work by some company.” “This may lead to a more formal development path for OSS.” “The companies will try to fragment the OSS movement through this path.”
 2. Testing is the key to robust software. Is there any reason to believe testing is looked upon as less of a bitter pill in the open source community?
 - “I do OSS development for glory and would not want to put my name to buggy software.” “Time pressures due to market demands work against testing in companies.” “Small scale testing by the developer herself does not help in OSS.”
 3. Are there software engineering methodologies followed in OSS development? Is it just code being exchanged and not documentation, specifications, etc.
 - “There are many exceptions in OSS. For Apache, processes were heavily documented.” “There is no one software engineering methodology that is followed uniformly either in CSS or OSS.” “Some OSS projects do, but the large majority don’t and they are run as an oligarchy.” “Significant data point is the peer review based PEP process used in Python development.”

Q&A Summary

4. Companies often claim some projects are open source, but all that they do is release the source code. They don't accept changes from the open community, and are not open about the development path.
 - “This is a serious concern in the OSS community.” “This will likely cause forks in the development path.”
5. What is the business case for OSS?
 - “There will be more businesses supporting OSS because their customers will demand solutions that are a mix of CSS and OSS.” “Consulting companies will reap money off OSS.” “The economic model for maintaining legacy OSS is tricky; look at Redhat yanking support for older version of its Linux.”

Results from Audience Poll

- Have you used OSS for your product/prototype development?
 - No, it leads to sub-standard products
 - No, because of legal issues
 - Yes, I use it almost solely
 - Yes, I use it somewhat
- Have you contributed to the OSS movement as a developer?
 - No, I have better uses for my time
 - No, because of company legal issues
 - No, it's on my ToDo list
 - Yes, I have



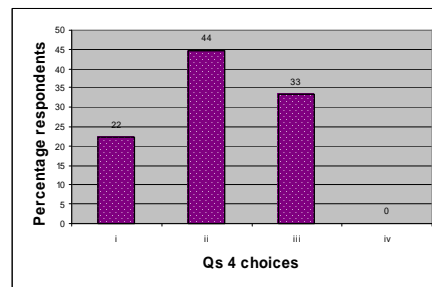
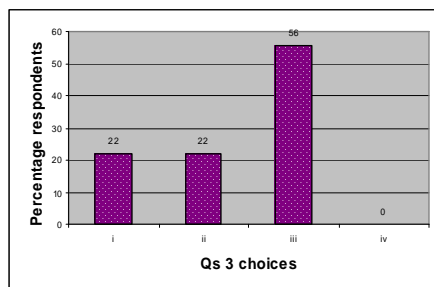
Panel: OSS & System Dependability

Slide 7/4

ISSRE '03: Denver, Colorado

Results from Audience Poll

- Do you think OSS based products are more reliable to natural failures?
 - No
 - Yes
 - Maybe
 - It doesn't matter
- Do you think OSS products are more hacker-proof than proprietary software?
 - No, I have better uses for my time
 - No, because of company legal issues
 - No, it's on my ToDo list
 - Yes, I have



Panel: OSS & System Dependability

Slide 8/4

ISSRE '03: Denver, Colorado