Open Source Security and Reliability

ISSRE 2002

Mike Shaver
Cluster File Systems / mozilla.org
<shaver@off.net>

Open Source & Open Development

Open source: Software licensing terms that provide specific rights to licensees. Trademark of the Open Source Initiative (www.opensource.org).

- free redistribution
- source availability
- modification (and distribution)

Open development: Organization-agnostic development methodology; usually combined with open source.

- public source trees
- public bug reporting
- public design and development discussion

Open Source Sales Pitch

- local control of source
  - "stripping down"
  - known-defect risk vs. change risk (unknown defect, administrative)
  - community self-support (esp. "unprofitable" communities)
    - solutions don't need to be universal
- choice of vendors/auditors for maintenance or verification
  - some protection against end-of-life/end-of-vendor
- wide visibility and analysis
- works with professionally/commercially-produced software

Open Development

- lightweight collaboration (existing infrastructure)
- almost never “anyone can check in”
- project management keyed to zero or more product cycles
- parallelization; part-time contribution
- visibility for project analysis

Some Challenges

- level of openness for sensitive defects
  - how do you share with the right people?
  - who are the "right" people?
- multiple distributors; synchronizing security updates
- supporting customized installations