

# FLOSS VS. PROPRIETARY SOFTWARE SECURITY

---

Mark Art, Carlos García

July 17, 2015

Technische Universität Berlin



1. Aims
2. Methodology
3. Technological view
4. Socioeconomic effects
5. Verdict
6. Q&A

1. Is FLOSS more secure than proprietary s/w?
2. Should businesses opt in for FLOSS or proprietary s/w out of security considerations?

- How to compare?
- What's *secure*? — hard to tell
- Metrics are often inconclusive
- FLOSS and proprietary software are interwoven
- Security may not be code-based
- Look at the common arguments

# TECHNOLOGICAL VIEW

## Open-source software is less secure because it's open

FLOSS is less secure because such projects' code is available to everyone and so everyone can spot bugs therein whereas proprietary software sources are "invisible"

## **Many eyes means more secure code**

Open-source code is more secure because its code is available to everyone for scrutiny

**If anyone can contribute then the code must be bad**

Anyone can add or modify existing code — poor coders too. Hence, poor coding skills bring about poor security.



## FLOSS quality assurance is weaker

FLOSS developers have less finances and resources than proprietary software vendors so their QA process is weaker.

## Proprietary s/w vendors are more trustworthy

When a vulnerability has been discovered, closed-source code software vendors have more resources to patch the issues

- No clear winner/loser
- Can't compare at the code level
- Need other inputs

# SOCIOECONOMIC EFFECTS

- Security issues are not just related to code and development process
- Decisions involve implementation or installation of software or services
- Customer awareness
- Vulnerability impact
- DCOM case

- Responsibility of vendors or developers
- Some companies offer this kind of service (RedHat)
- Common practice: End-of-Life software

- Regularity of security patches by vendors or developers
- Significance of security fixes: issues fixed with a patch
- Scheduling guidelines + comprehensive patch management program

- N/A up to a year or more (need to test before release)
- Availability: May need to wait till the next major release or service pack
- With FLOSS — fix and implement the changes immediately



- Custom builds create their own potential vulnerabilities
- Not every open-source product is reviewed by security experts

VERDICT

**Q:** Is FLOSS more secure than proprietary s/w?

**A:**

**Q:** Is FLOSS more secure than proprietary s/w?

**A:** No. Both are "insecure".

**Q:** Should businesses opt in for FLOSS or proprietary s/w out of security considerations?

**A:**

**Q:** Should businesses opt in for FLOSS or proprietary s/w out of security considerations?

**A:** It depends.

Q & A