Open Source Software (OSS) and Security

David A. Wheeler
March 15, 2004

This presentation contains the views of the author and does not indicate endorsement by IDA, the U.S. government, or the U.S. Department of Defense.

Outline

- **Extreme claims**
- **Open design: A security fundamental**
- **Problems with hiding source & vulnerability secrecy**
- **Proprietary advantages… not necessarily**
- **Common criteria evaluation challenges**
- **OSS bottom line**

Extreme claims

- **Extreme claims**
  - **“OSS is always more secure”**
  - **“Proprietary is always more secure”**
- **Reality: Neither OSS nor proprietary always better**

Open design: A security fundamental

- **Saltzer & Schroeder [1974/1975] - Open design principle**
- **OSS better fulfills this principle**
- **Security experts perceive OSS advantage**
  - **Bruce Schneier, Vincent Rijmen (AES), Whitfield Diffie, ...**

Problems with hiding source & vulnerability secrecy

- **Hiding source doesn't halt attacks**
  - **Dynamic attacks**
  - **Static attacks (binaries, disassemblers, decompilers)**
  - **Can't keep source secret**
  - **Inhibits help**
- **Vulnerability secrecy doesn't halt attacks**
  - **Rediscovery**
  - **Days works, not years**

Proprietary advantages… not necessarily

- Experienced developers who understand security produce better results
- Proprietary developers higher quality?
- No guarantee OSS is widely reviewed

Common Criteria and OSS

- Common Criteria (CC) can be used on OSS
- CC matches OSS imperfectly
- Government policies discriminate against OSS

OSS bottom line

- **OSS security preconditions**
  - **Developers/reviewers need security knowledge**
    - **Knowledge more important than licensing**
  - **People have to actually *review* the code**
  - **Problems must be fixed**
- **OSS: less secure, later more secure (~yr)**
- **Neither OSS nor proprietary always better**

Detailed Slides

Outline

- Extreme claims
- Open design: A security fundamental
- Problems with hiding source & vulnerability secrecy
- Proprietary advantages… maybe
- Common criteria evaluation challenges
- OSS bottom line

Extreme claims

- **Extreme claims**
  - **“OSS is always more secure”**
  - **“Proprietary is always more secure”**
- **Reality: Neither OSS nor proprietary always better**

Open design: A security fundamental

- **Saltzer & Schroeder [1974/1975] - Open design principle**
  - **the protection mechanism must not depend on attacker ignorance**
- **OSS better fulfills this principle**
- **Security experts perceive OSS advantage**
  - **Bruce Schneier: “demand OSS for anything related to security”**
  - **Vincent Rijmen (AES): “forces people to write more clear code & adhere to standards”**
  - **Whitfield Diffie: “it’s simply unrealistic to depend on secrecy for security”**

Problems with hiding source & vulnerability secrecy

- **Hiding source doesn't halt attacks**
  - **Dynamic attacks don't need source or binary**
  - **Static attacks can use pattern-matches against binaries, disassembled & decompiled results**
  - **Presumes you can keep source secret**
    - **Attackers may extract or legitimately get it**
  - **Secrecy inhibits those who wish to help, while not preventing attackers**
- **Vulnerability secrecy doesn't halt attacks**
  - **Vulnerabilities are a time bomb and are likely to be rediscovered by attackers**
  - **Brief secrecy works (10-30 days), not years**

Proprietary advantages… not necessarily

- **Experienced developers who understand security produce better results**
  - **Experience & knowledge *are critical*, but...**
  - **OSS developers often very experienced & knowledgeable too (BCG study: average 11yrs experience, 30 yrs old)**
- **Proprietary developers higher quality?**
  - **Dubious; OSS often higher reliability**
  - **Market rush impairs proprietary quality**
- **No guarantee OSS is widely reviewed**
  - ***True!*** **& unreviewed OSS may be very insecure**
  - **Also true for proprietary (rarely reviewed!)**

Common Criteria and OSS

- **Common Criteria (CC) can be used on OSS**
  - **Red Hat Linux, SuSE Linux (FIPS 140-2: OpenSSL)**
- **CC matches OSS imperfectly**
  - **CC developed before rise of OSS**
  - **Doesn't credit mass peer review or detailed code review**
  - **Requires mass creation of documentation not normally used in OSS development**
- **Government policies discriminate against OSS**
  - **Presume that vendor will pay hundreds of thousands or millions for a CC evaluation ("big company" funding)**
    - **Presumes nearly all small business & OSS insecure**
  - **Presume that "without CC evaluation, it's not secure"**
  - **Need to fix policies to meet real goal: secure software**
    - **Government-funded evaluation for free use/support?**
    - **Multi-Government funding?**
    - **Alternative evaluation processes?**

OSS bottom line

- **OSS security preconditions**
  - **Developers/reviewers need security knowledge**
    - **Knowledge more important than licensing**
  - **People have to actually *review* the code**
    - **Reduced likelihood if niche/rarely-used, few developers, rare computer language, not really OSS**
    - **More contributors, more review**
  - **Problems must be fixed**
- **OSS: less secure, later more secure (~yr)**
  - **Borland InterBase/Firebird (user: politically)**
- **Neither OSS nor proprietary always better**

Backup Slides

Basics of Open Source Software (OSS) / Free Software (FS)

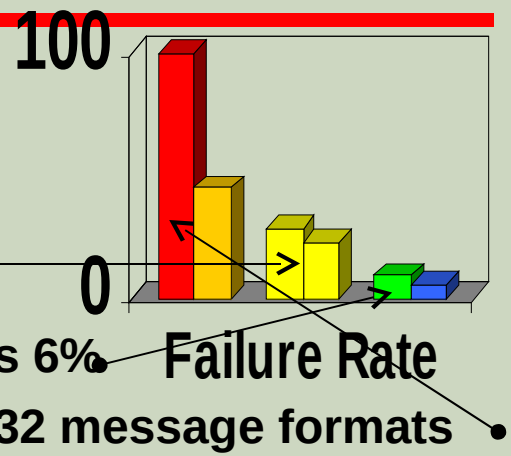
- **Open Source Software / Free Software (OSS/FS) programs have licenses giving users the freedom:**
  - **to run the program for any purpose,**
  - **to study and modify the program, and**
  - **to freely redistribute copies of either the original or modified program (without royalties, etc.)**
- ***Not* non-commercial, *not* necessarily free-of-charge**
  - **Often supported via commercial companies**
- **Synonyms: Libre software, FLOS software (FLOSS)**
- **Antonyms: proprietary software, closed software**

Extreme claims (and counterexamples)

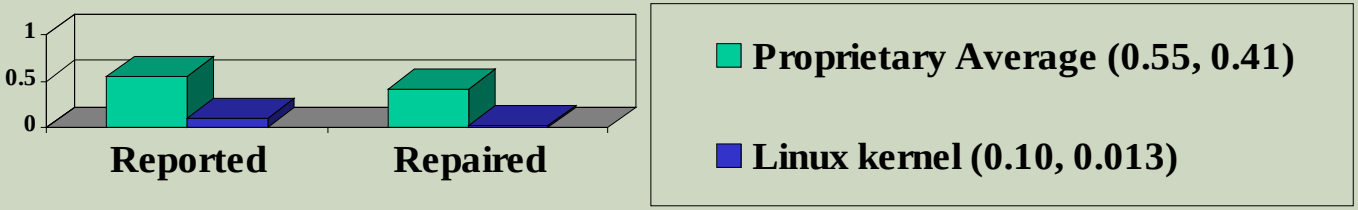
- **"OSS is always more secure"**
  - **Counterexample: Sendmail**
- **"Proprietary is always more secure"**
  - **Counterexample: Windows & IIS**
  - **Vulnerabilities: Apache 0, IIS 8 over 3yrs**
  - **J.S. Wurzler hacker insurance costs 5-15% more for Windows than for Unix or Linux**
  - **Windows websites more vulnerable**

Category	Proprietary	OSS/FS
Defaced	**66% (Windows)**	**17% (GNU/Linux)**
Deployed Systems	**49.6% (Windows)**	**29.6% (GNU/Linux)**
Deployed websites (by name)	**24.81% (IIS)**	**66.75% (Apache)**

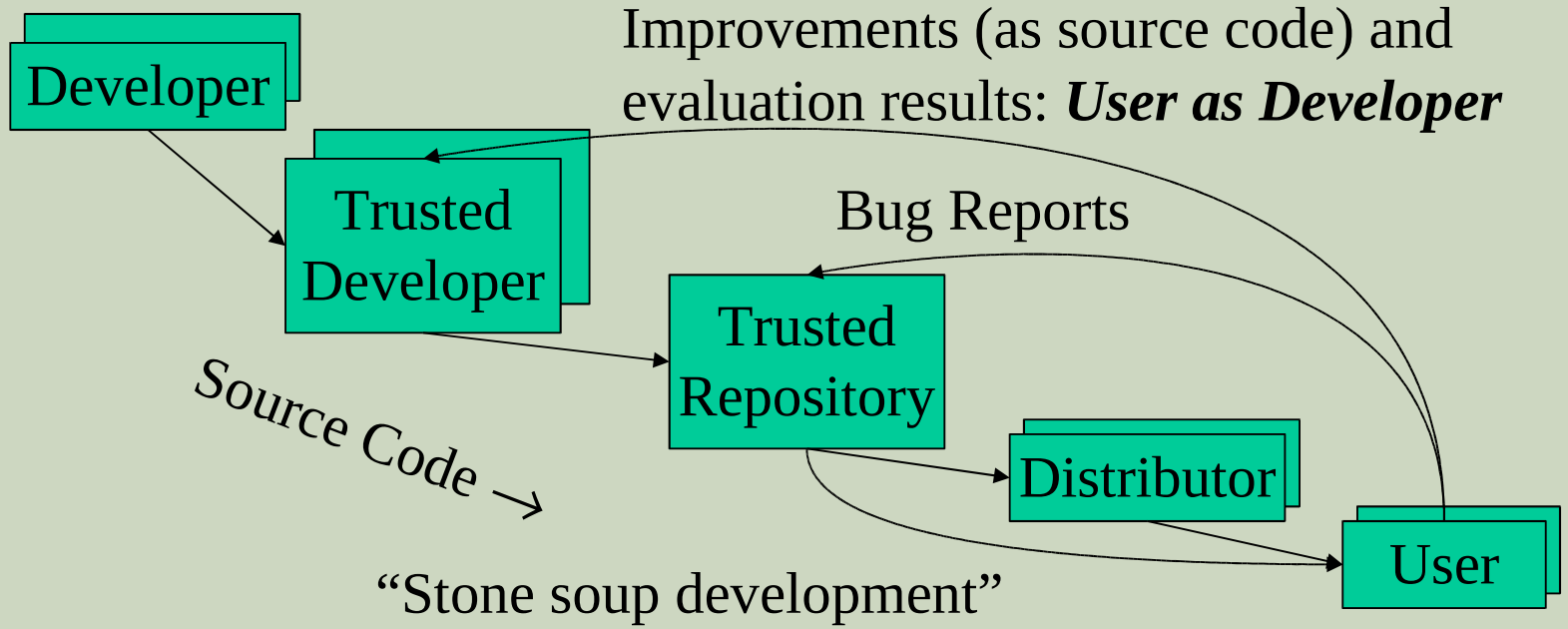
Reliability



- Fuzz studies found OSS/FS apps significantly more reliable [U Wisconsin]
  - Proprietary Unix failure rate: 28%,23%
  - OSS/FS: Slackware Linux 9%, GNU utilities 6%
  - Windows: 100%; 45% if forbid certain Win32 message formats
- GNU/Linux vs. Windows NT 10 mo study [ZDNet]
  - NT crashed every 6 weeks; both GNU/Linuxes, never
- IIS web servers >2x downtime of Apache [Syscontrol AG]
- Linux kernel TCP/IP had smaller defect density [Reasoning]



OSS/FS Development Model



- OSS/FS users typically use software without paying licensing fees
- OSS/FS users typically pay for training & support (competed)
- OSS/FS users are responsible for developing new improvements & any evaluations that they need; often cooperate/pay others to do so

Acronyms

- COTS: Commercial Off-the-Shelf (either proprietary or OSS)
- DoD: Department of Defense
- HP: Hewlitt-Packard Corporation
- JTA: Joint Technical Architecture (list of standards for the DoD); being renamed to DISR
- OSDL: Open Source Development Labs
- OSS: Open Source Software
- RFP: Request for Proposal
- RH: Red Hat, Inc.
- U.S.: United States

Interesting Documents/Sites

- **“Why OSS/FS? Look at the Numbers!” http://www.dwheeler.com/oss_fs_why.html**
- **“Use of Free and Open Source Software in the US Dept. of Defense” (MITRE, sponsored by DISA)**
- **President's Information Technology Advisory Committee (PITAC) -- Panel on Open Source Software for High End Computing, October 2000**
- **“Open Source Software (OSS) in the DoD,” DoD memo signed by John P. Stenbit (DoD CIO), May 28, 2003**
- **Center of Open Source and Government (EgovOS) http://www.egovos.org/**
- **OpenSector.org http://opensector.org**
- **Open Source and Industry Alliance http://www.osaia.org**
- **Open Source Initiative http://www.opensource.org**
- **Free Software Foundation http://www.fsf.org**
- **OSS/FS References http://www.dwheeler.com/oss_fs_refs.html**