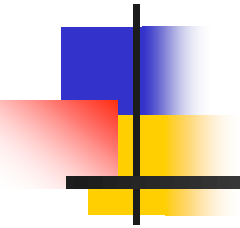

CSE 543

Information Assurance in Open Source Software

Professor Stephen S. Yau

Spring, 2014

Open-Source Software

- Open source software (OSS) is software whose ***source code and certain rights*** normally reserved for copyright holders are ***freely available to the public for redistribution, modification and examination***
- OSS has become more and more popular due to
  - ***Internet*** which supports easy access to diverse software source codes and massive communications among interactive OSS communities
  - Various ***software development tools*** which help OSS development are available (e.g. version control systems, bug tracking systems, testing tools, package management systems)
  - Prevent predatory ***vendor lock-in*** (the situation in which customers are dependent on a single vendor for some products. Vendor lock-in may grant the vendor some extent of monopoly power.)

Examples of OSS

- Apache HTTP Server (http://httpd.apache.org/) (web server)
- GNOME (http://www.gnome.org/) (Linux desktop environment)
- GNU Compiler Collection (http://www.gnu.org/software/gcc/gcc.html) (GCC, a suite of compilation tools for C, C++, etc)
- KDE (http://www.kde.org/) (Linux desktop environment)
- Mozilla (http://www.mozilla.org/) (web browser and email client)
- Firefox (http://www.mozilla.com/en-US/firefox/) (web browser based on Mozilla)
- MySQL (http://www.mysql.com/) (database)
- OpenOffice.org (http://www.openoffice.org/) (office suite, including word processor, spreadsheet, and presentation software)
- PHP (http://www.php.net/) (web development)
- Ruby(http://www.ruby-lang.org/) (programming language)

Characteristics of Open Source Software Development

- ***Collaborative development*** in public open communities
- ***Sharing*** ideas, technologies and expertise
- Distributed and independent ***peer reviews***
- Better quality and higher reliability through ***rapid discovery*** of vulnerabilities and ***quick fixes***
- ***Lower*** development cost
- Users treated as ***co-developers,*** reporting bugs and providing bug fixes.
- ***Early releases*** - increasing chances of finding co-developers early.

Characteristics of Open Source Software Development (cont.)

- ***Frequent integration*** – since components of OSS are developed in a distributed manner (by multiple developers in different locations), integration of the components should be done as often as possible during the development in order to avoid overhead of fixing a large number of bugs at the end
- ***Multiple versions*** with different features
- ***Beta versions*** with latest features and risks of having more vulnerabilities
- ***Stable versions*** with fewer features that have been thoroughly tested.
- ***High modularization*** **-** The general structure of OSS is modular allowing parallel development on independent components.
- ***Flexible structure*** – The structure of OSS is flexible enough to adopt new or changing user requirements during development or after release.

Open Source Initiative (OSI)

- Open Source Initiative (OSI) (http://www.opensource.org/) is a non-profit organization founded in 1998 by Netscape Communications Corporation
  - Dedicated to promoting OSS
  - Build bridges among different constituencies in open source community.
  - Educates developers, decision makers and users about the advantages of OSS and OSS development techniques and technologies - Education Committee (http://www.opensource.org/osi-open-source-education)
- Established the Open Source Definition (OSD) (http://www.opensource.org/docs/osd)

Open Source Definition

- Free redistribution and must include ***source code***.
- ***Integrity*** of The Author's Source Code
- The license
  - Must ***allow modifications, derived works***, and to be distributed under same terms of the license of the original software.
  - No discrimination against *persons or groups*.
  - No discrimination against ***fields of endeavor***.
  - Must not be specific to a product
  - Must not restrict other software
  - Must be technology-neutral

Open Source Licensing

- There are many open source licenses.
  - The license list approved by OSI is at http://opensource.org/licenses/alphabetical

    (e.g. Educational Community License, Academic Free License, IBM Public License, Intel Open Source License, Microsoft Public License, Mozilla Public License)
- Choosing the right license for software is important.
- All open source licenses have to be submitted for approval by the OSI

OSS vs. Freeware or Shareware

- ***Freeware*** refers to software available for ***use at no cost***
- ***Shareware*** refers to software ***provided to users without payment on a trial basis*** and ***often limited by functionality or time of use***.
- OSS vs. Freeware or Shareware
  - OSS
    - OSS does not restrict any party from ***modifying and redistributing*** the original software
    - OSS does ***not restrict any party from selling the software as a component*** of an aggregate software. The license shall not require a royalty or other fee for such sale.
  - Freeware or Shareware
    - Developers are holding the software copyrights
    - ***Proprietary and closed source code***
    - The license ***restricts modifications and redistributions*** of the software

Business Perspectives of OSS

- Most software companies do not disclose their source code and do sell their software without source code
- Some companies are willing to contribute to OSS because OSS can
  - ***Achieve greater penetration of the market***. Companies offering open source software may establish an industry standard, and thus gain competitive advantage
    - Almost every global standard on web technology (Java, Perl, PHP, TCL) has been based on open source technology
  - ***Reduce cost*** for
    - ***Research and development***
    - ***Marketing and logistical services***
  - ***Speed up delivery*** of new products

Business Perspectives of OSS (cont.)

- Help companies in the following aspects:
  - Keep abreast of software technology development
  - Promote a company's reputation, including its commercial products
  - Help companies produce reliable, high quality software quickly and inexpensively
  - Potential for a more flexible technology and quicker innovation
  - Generate revenue from ancillary services like technical support, consulting, tutorials, training and publications.

OSS Market

- Worldwide revenue from OSS is expected to reach €57 billion by 2020*
- Large software vendors, like IBM, Dell, Google, HP, and Oracle, are also making significant amounts of indirect revenue from their activities with and support of OSS

- http://www.statista.com/statistics/270805/projected-revenue-of-open-source-software-since-2008/

Major OSS Companies

- Red Hat: Operating system - Linux
- Untangle: gateway that blocks spam, spyware, viruses and adware
- WordPress: Blogging platform
- OpenBravo: Enterprise resource planning (ERP)
- JasperSoft: Business Intelligence (BI) Suite
- Canonical: Desktop operating system - Ubuntu Linux
- SugarCRM: Customer relationship management (CRM)
- Digium: IP telephony platform
- MySQL: Database
- Mozilla Foundation: Web browser
- Apache Software Foundation: Web server

Debate on Security of OSS

- OSS is ***less secure***
  - ***Difficult to control the quality*** of software.
  - ***No or very little responsibility*** for developers
  - Source code ***available to attackers***
  - Simply making source code available does ***not guarantee review***
  - A ***malicious developer*** can also participate in OSS development
  - OSS often has problems with ***poor documentation***
  - Open source ***development process may not be well defined*** and the stages in the development process, such as system testing and documentation, ***may be ignored***

Debate on Security of OSS (cont.)

- OSS is ***more secure***
  - Commonly used OSS is ***often more reliable***
  - Programmers tend to write OSS code ***more carefully for reputation***
  - Open communications among programmers of OSS allow them to have ***more knowledge for security issues and technologies***
  - An attacker usually runs the program, sends the input to the program, and finds if its response indicates it contains any security vulnerability. ***No difference between open and closed programs for an attacker to find security vulnerabilities*** in the program with or without source code.
  - If a user wants to know whether a particular feature is secure or to find malicious functions, viruses or worms, the user can find it by ***examining the source code***
  - Closed software is expected to be more secure because of the secrecy of its source code. However, security through obscurity is not working because ***keeping vulnerabilities secret does not make the vulnerabilities go away***

Debate on Security of OSS (cont.)

- OSS is ***more secure*** ***(cont.)***
  - For proprietary software, users are forced to accept the level of security the vendors have chosen to provide. However, for OSS, ***users can choose the security level*** as high as they want by adding more security features.
  - OSS can be ***developed according to purely technical requirements***, and does not require developers to think about commercial pressure (cost and time-to-market) that often degrades the quality of the software.
    - Commercial pressures make software developers pay more attention to customers' requirements than to security requirements since such features are somewhat invisible to the customer

OSS or Proprietary Software?

- Which software, OSS or proprietary software, is more secure?
  - No answer.
  - Decide which software you will use carefully based on your business goals, context, budget, and requirements.
  - If you decide to use OSS, you need to plan ahead carefully to use it securely