RESEARCH REVIEW JOURNALS
Volume-03
Issue-10
October-2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

Importance of Open Source Software

Shaveta

Assistant Professor, Department of Computer Science &Applications, Guru Nanak College, Ferozepur, Punjab (India)

ARTICLE DETAILS

Article History
Published Online: 10 October 2018

Keywords
Open Source Software

ABSTRACT

Open source software is computer software that has a source code available to the general public for use as is or with modifications. This software typically does not require a license fee. One of the major reasons for this breach of security has been attributed to proprietary software whose source is available only to the company which made it. Thus you have no surety that the proprietary and pre-compiled software has no hole to help an individual break security of your computer or network.

1. Introduction

Open source software is unique in that it is always released under a license that allows users to access, modify and redistribute the source code. Source code is a specialized language that allows software developers to create and modify computer programs. If you do not have legal access to the source code, then the program cannot be changed or moved to a different kind of computer.

Open-source software may be developed in a collaborative public manner. According to scientists who have studied it, open-source software is a prominent example of open collaboration. The term is often written without a hyphen as "open source software". open source software is freely accessible.

Open-source software development, or collaborative development between multiple independent contributors, generates an increasingly more diverse scope of design perspective than any company is capable of developing and sustaining long term. A 2008 report by the Standish Group states that adoption of open-source software models has resulted in savings of about $60 billion (£48 billion) per year to consumers.

Security of an information system depends upon its design and the components used for building it. Apart from the hardware, the major components i.e. brain of a computer or digital system is software. Therefore, how this software is written is a major deciding factor in determining the security of a digital system, be it a piece of code for some ROM, an operating system for a network device like a router or just an application like a web browser.

2. History

- In the early days of computing, programmers and developers shared software in order to learn from each other and evolve the field of computing. Eventually, the open-source notion moved to the way side of commercialization of software in the years 1970-1980. However, academics still often developed software collaboratively, for example Donald Knuth in 1979 with the TeX typesetting system[8] or Richard Stallman in 1983 with the GNU operating system. In 1997, Eric Raymond published The Cathedral and the Bazaar, a reflective analysis of the hacker community and free-software principles. The paper received significant attention in early 1998, and was one factor in motivating Netscape Communications Corporation to release their popular Netscape Communicator Internet suite as free software.
- The new term they chose was "open source", which was soon adopted by Bruce Perens, publisher Tim O'Reilly, Linus Torvalds, and others. The Open Source Initiative was founded in February 1998 to encourage use of the new term and evangelize open-source principles.
- While the Open Source Initiative sought to encourage the use of the new term and evangelize the principles it adhered to, commercial software vendors found themselves increasingly threatened by the concept of freely distributed software and universal access to an application's source code. A Microsoft executive publicly stated in 2001 that "open source is an intellectual property destroyer. I can't imagine something that could be worse than this for the software business and the intellectual-property business."[11] However, while Free and open-source software has historically played a role outside of the mainstream of private software development, companies as large as Microsoft have begun to develop official open-source presences on the Internet. IBM, Oracle, Google and State Farm are just a few of the companies with a serious public stake in today's competitive open-source market. There has been a significant shift in the corporate philosophy concerning the development of FOSS.
- The free-software movement was launched in 1983. In 1998, a group of individuals advocated that the term free software should be replaced by open-source software (OSS) as an expression which is less ambiguous and more comfortable for the corporate world.[16] Software developers may want to publish their software with an open-source license, so that anybody may also develop the same software or understand its internal functioning. With open-source software, generally anyone is allowed to create

modifications of it, port it to new operating systems and instruction set architectures, share it with others or, in some cases, market it.

- The Open Source Definition, notably, presents an open-source philosophy, and further defines the terms of use, modification and redistribution of open-source software. Software licenses grant rights to users which would otherwise be reserved by copyright law to the copyright holder. Several open-source software licenses have qualified within the boundaries of the Open Source Definition. The most prominent and popular example is the GNU General Public License (GPL), which "allows free distribution under the condition that further developments and applications are put under the same license, thus also free

3. How is open source software useful to small business?

- If you were to review information on open source software you will find many different claims and counterclaims with respect to its advantages and limitations. Some of the differing opinions arise from the fact that while an open source software package may work very well in one business environment, it might not work so well in a different environment. Depending on your current system (i.e. what software you are using now), your business needs and the open source product you choose (some are better than others) certain advantages of using open source software will vary. The second development was the invention of high-speed computer networks. Local-area networks or LANs allow hundreds of machines within a building to be connected in such a way that small amounts of information can be transferred between machines in a few microseconds or so. Larger amounts of data can be Distributed Computing become popular with the difficulties of centralized processing in mainframe use.

4. Security

Security of an information system depends upon its design and the components used for building it. Apart from the hardware, the major components i.e. brain of a computer or digital system is software. Therefore, how this software is written is a major deciding factor in determining the security of a digital system, be it a piece of code for some ROM, an operating system for a network device like a router or just an application like a web browser.

- While considering the role for home users, computers and digital systems like mobile phones, PDAs etc. have changed dramatically the way we live our lives. Most of the information that used to be only on paper or in hard files is now shared on the computers and the Internet. Be it the accounting information of its customers by bank, transactions history for online banking, examination results of its students by a university or college, sensitive records of police, armed forces, etc. almost everything finds its way to a computer fileThe minicomputer model may be used when resource sharing (Such as sharing of information databases of different types, with each type of database located on a different machine) with remote users is desired.

- Not only this, we use computers and the Internet for email, instant messaging and voice communication. Moreover, land mobile phones are connected to theInternet. Even small household items like oven, refrigerators, washing machines, etc. are expected to be networked and connected to the Internet in very near future. Internet. Even small household items like oven, refrigerators, washing machines, etc. are expected to be networked and connected to the Internet in very near future.

- With this proliferation of computers everywhere, new methods have been invented to break into computers and use the gained information to the intruder's advantage and according to a survey, some even think that the Internet is a conspiracy by an alien society to get into our sociological structure.

- While computer and internet security might not be as important from the perspective of a home user, it is of tremendous value for small businesses, corporate and multinational companies, governments, military, etc. where millions and billions of rupees or dollars or even state secrets are at stake. Consider a bank's security system being compromised and money being transferred to some other account in some other bank. Or imagine a scence where a nuclear plants control system is taken over.

- These are only known and reported incidents. There may be many such episodes which have not been made public. Banks do not publicize their break-ins so as not to damage their reputation. Governments do not discuss these issues in public as not to demoralize their people.

5. Advantages of open source security

Though there are many, main points and the merits are described below

- When a software code is open to be seen and evaluated by everyone, the developer and programmer takes every care to make it nice, clean and secure because reputation of the programmer is at stake. If there are mistakes and errors left in the code, the whole developers community is out there to discover it. There is no such concept with closed programs.

- If the software code is made secret, only crackers and attackers discover the holes and they would seldom publicize them i.e. only the bad guys discover mistakes and if there are not publicized, there are no fixes for them too. Whereas in the case of open

source software, good guys also get a chance to discover the mistakes and then apply fixes to them.

- Finding and fizing vulnerabilities and errors in popular software is one way for open source programmers to earn the respect of their peers and the community. Therefore, it provides some motivation to examine source code and improvise upon it.

- Because it is open to change from everybody, open source software is very diverse in nature. For example, there are many Unix like operating systems, like, Linux, Solaris, OpenBSD, FreeBSD, etc. Further, Linux has many of its own distributions. Therefore, it is not a good choice for crackers and writers of viruses and malware. It is because of this reason that there has seldom been a case of Linux, Unix or other open source software virus of worm as against the case of proprietary Windows for which multitude of viruses are available and keep surfacing every other day.

- Companies that try to keep their source code secret run into the risk that someone might access the source code, find bugs and exploit them sometimes without letting the company know it. Examples of software being taken away by hackers already exist [24]. CISCO's network was compromised and almost 800 MB of source code was taken away. In a similar episode, source code Miscrosoft Windows was taken away by hacker

6. Source code scanning tools

The best way to ensure that a software is free of errors and vulnerabilities is to make a manual audit of the code. However, the process may be time consuming and long enough to be impractical for projects involving length code. There are many automated tools available to scan a piece of code for any possible errors particularly those which are documented and quite common. Both proprietary and open source tools are available for this purpose. Some of these valuable open source tools are described below:

- Lint is one of the oldest tool which checks inconsisties and errors in the C code. A similar tool called nslint checks errors in DNS files and another tool weblint checks errors in HTML files. A similar source code scanner for C++ code is client. Pscan and Cqual are similar tools that scan C source code for inconsistencies.

- BOON is a tool that can find buffer overflow possibilities in C programs. MOPS finds vulnerabilities in C programs and checks whether a program conforms to paradigm of secure programming.

7. Key points to remember open source system

1. Open source software is computer software that has a source code available to the general public for use as is or with modifications. This software typically does not require a license fee.

2. All the things related to security described are serious issues and need to be addressed. To make our computer systems more secure we need to make the software that it runs, more reliable and free of errors and bugs.

8. Conclusion

We have discussed the two philosophies of software development with respect to keeping them secure and not prone to exploits. Each of these has its own merits and demerits. However, as we have seen, open source paradigm has far more benefits than the secret code paradigm which may allow a company to leave a hole or backdoor for later exploit. Particularly, for Pakistan, the open source model provides many benefits in the form of free software along with transfer of technology i.e. source code for our review and modification which should result in better security for our IT infrastructure.

References

1. Auchard, Eric, "Phones, Car Engines Face Security Threats", Yhaoo News, as on 09-02-2005 **
2. Fleish, Brett D., "Grand Research Challenges in IT Security and Assurance", Proceedings of International Workshop On Frontiers of Information Technology, 2003. [3] Folkert, "Tools and Tips For Auditing Code", http://www.vanheusden.com/Linux/audit.html as on 13-08-2005.
3. Gaudin, Sharon, "India/Pakistan Virus Writers Take War Online" http://www.esecurityplanet.com/trends/print.php/2109031 as on 17-05-2005 **
4. Ibrahim, Aazar and Hussain, Mukhtar, "Net-centric Organizations in Pakistan: Security and protection of IT infrastructure", Proceedings of International Workshop On Frontiers of Information Technology, 2003.
5. Jabeen, Farhana, "Internet and Pakistani Society", Proceedings of International Workshop On Frontiers of Information Technology, 2003.
6. Jabeen, Farhana and Sheri, Muqeem Ahmad, "Security Threats in Peer-to-Peer Technology", Proceedings of International Workshop On Frontiers of Information Technology, 2003.
7. Kamel, Ibrahim, "On Connecting Smart Appliances to the Internet", Proceedings of International Workshop On Frontiers of Information Technology, 2003.
8. Kamel, Ibrahim, "IT Security: The Next Frontier", Proceedings of International Workshop On Frontiers of Information Technology, 2004.
9. Knight, Will, "FBI Trojan Horse Triggers Alarms", NewScientist http://www.newscientist.com/article.ns?id=dn1608&& print=true as on 17-05-2005 **
10. Lateef, Khalid, "Challenges in Embedded System's Security", Proceedings of International Workshop On Frontiers of Information Technology, 2003. [12] Leyden, John, "CIA Plays

Cyber War Games", The Register, May 2005, http://www.theregister.co.uk/2005/05/27/cia_cyberwar _game/ as on 13-08-2005. [13] Leyden, John, "Failing UK Cyber Defenses Need Overhaul", The Register, http://www.theregister.co.uk/2005/04/27/niscc_reform/ print.html as on 17-05-2005**

11. Lions, L.J. "Report by the Inquiry Board, Ariane 5 Flight 501 Failure, Technical Report", European Space Agency, 1996.
12. Maqsood, Sadiq, "Hackers Block Government's Computer Network", Business Recorder, 2002. **
13. Moore, Matt, "Some Fear Virus Threat To Cell Phones.
14. Nazario, Jose, "Source Code Scanners for Better Code", Linuxjournal, http://www.linuxjournal.com/article/5673 as on 13-08-2005. **
15. Perens, Bruce, "Why Security-Through-Obscurity Won't Work", Slashdot, http://slashdot.org/features/980720/0819202.shtml as on 13-08-2005
16. Poulsen, Kevin, "Sluggish Movemnet on Power Grid Cyber Security", The Register, August 2004.
17. http://www.theregister.co.uk/2004/08/16/power_grid_c ybersecurity/ as on 13-08-2005.
18. Poulsen, Kevin, "Slammer Worm Crashed Ohio Nuke Plant", The Register, August 2003, http://www.theregister.co.uk/2003/08/20/slammer_wor m_crashed_ohio_nuke/ as on 13-08-2005.
19. Sullivan, Bob, "Cell Phone Voicemail Easily Hacked", MSNBC as on 28-02-2005**
20. WWW, "Open Source Software and Security" http://www.oss-watch.ac.uk/resources/security.xml as on 13-08-2005. **
21. Whitlock, Natalie, "The Security Implications of Open Source Software", IBM, March 2001.
22. Zhen, Jian, "Insecurity Through Obscurity", Computerworld, http://www.computerworld.com/printthis/2005/0,4814, 102307,00.html as on 13-08-2005.

