INSTITUTE FOR DEFENSE ANALYSES

What is Open Security?

David A. Wheeler

August 21, 2013
IDA Non-Standard Document
NS D-4993
Log: H 13-001186
Copy

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

About This Publication

This work was conducted by the Institute for Defense Analyses (IDA) under contract N66001-11-C-0001, subcontract D6384-S5, "Homeland Open Security Technology (HOST)," for Georgia Tech Research Institute. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

What is Open Security?

David A. Wheeler

August 21, 2013

INSTITUTE FOR DEFENSE ANALYSES

This document provides a definition of the term "open security,"
along with some background, clarifications, and discussion.

Various government projects work to enable "open security" – but what does that term mean? This article proposes an answer, along with background, clarifications, and discussion.

Proposed Definition

Open security is the application of open source software (OSS) approaches to help solve cyber security problems. OSS approaches collaboratively develop and maintain intellectual works (including software and documentation) by enabling users to use them for any purpose, as well as study, create, change, and redistribute them (in whole or in part). Cyber security problems are a lack of security (confidentiality, integrity, and/or availability), or potential lack of security (a vulnerability), in computer systems and/or the networks they are a part of.

In short, open security improves *security* through *collaboration*.

Background

Modern society depends on computer systems for a myriad of functions, yet cyber security weaknesses enable attackers to subvert those computer systems. Often attackers have the advantage—attackers can typically exploit systems by finding one or a few weaknesses, while defenders must eliminate or remediate a large number of potential vulnerabilities in large, complex systems.

In recent years OSS approaches have enabled widespread collaboration and produced high-quality, widely used products. Widely used OSS programs include Linux (a key part of Android), the Apache web server, and the Firefox web browser. OSS approaches have proven themselves in areas beyond software, e.g., Wikipedia uses OSS approaches to develop and maintain a remarkable encyclopedia.

Since OSS approaches have proven themselves useful in solving other problems, it seems reasonable to believe that OSS approaches could help solve some cyber security problems as well.

Defenders working together to eliminate and remediate vulnerabilities are likely to be far more effective than if they work in isolation. For example, defenders as a group can be more innovative and more thorough, since with OSS approaches many different ideas can be quickly combined together. OSS approaches are not free of cost, but since they often cost nothing to license and support can be competed, OSS solutions are often inexpensive and thus more likely to be used.

This is not to say that all solutions must necessarily be OSS, or that OSS approaches can solve all cyber security problems. However, OSS approaches have much to offer in resolving current cyber security problems.

Clarifications

Open security is simply the application of OSS approaches to a particular type of problem, so it builds on existing OSS approaches. People must be allowed to legally collaborate, so:

- When applied to software, this proposed definition requires that software be released to users with rights that meet the Open Source Definition [OSI] as maintained by the Open Source Initiative (OSI), as well as the Free Software Definition [FSF] as maintained by the Free Software Foundation (FSF). Both the OSI and FSF perform legal reviews to determine whether licenses meet these definitions; such licenses include the Massachusetts Institute of Technology (MIT) license, the Apache 2.0 license, the GNU Lesser General Public License (LGPL), and the GNU General Public License (GPL).

- When applied to other works (such as documentation), this proposed definition requires works to meet the Definition of Free Cultural Works [FreedomDefined]. This definition is used, for example, by the WikiMedia Foundation [WikiMedia]. Such content is often called "open content" (though that term has many meanings). Works that meet this definition include those released under the Creative Commons Attribution (CC-BY) and Attribution-ShareAlike (CC-BY-SA) licenses. Works that do not meet this definition include those released under the Creative Commons "non-commercial" licenses (which forbid commercial use) and "no-derivative" licenses (which forbid further collaboration) [Creative Commons].

Intellectual works that have no copyright (e.g., a "work of the U.S. government" as defined in 17 USC 101) may provide these freedoms. When they do, OSS approaches can also be applied to them.

Legally allowing collaboration is only the first step—the next is to actually collaborate. There are many different ways to collaborate, and many tools that support it, but these can be varied depending on the needs of the collaborators.

Discussion

The definition of open security could have been narrowed to apply only to software, or broadened to include work whose receivers have fewer rights. These alternatives were rejected for the following reasons:

- A software-only definition excludes collaborative development of other helpful materials, such as documentation to help developers write better software. Indeed, typical definitions of "software" include some kinds of documentation. There seems to be no strong reason to use a narrower definition, and many reasons to use an inclusive one.

- A definition that eliminates some of these rights would eliminate the ability, or many of the incentives, to collaborate.

The open security definition is derived from the free software definition, because that definition is much shorter and simpler than the open source definition (the most likely alternative). Formal U.S. Government definitions, such as the definition in the U.S. DoD 2009 policy [DoD2009], also use the free software definition as their starting point.

This definition of open security does not exclude "open hardware" per se, but the definition of the term "open hardware" is still in flux at the time of this writing. Additionally, the current focus in the open security community is more on improving software and related documentation and less on hardware. Thus, it seems appropriate to focus the definition and discussion on the better-understood areas, without excluding hardware in the future.

Conclusions

Simply defining the term "open security" does not solve cyber security problems. However, a clear definition of "open security" makes it easy to determine whether an approach is, or is not, open security.

Since open security approaches have the potential to help solve serious problems, a clear definition will help people focus on determining where open security approaches can be best applied.

References

[Creative Commons] Creative Commons. *About The Licenses*. http://creativecommons.org/licenses/

[DoD2009] Department of Defense (DoD). *Clarifying Guidance Regarding Open Source Software (OSS)*. 2009-10-16. http://dodcio.defense.gov/Portals/0/Documents/FOSS/2009OSS.pdf

[FreedomDefined] Freedom Defined. *Definition of Free Cultural Works*.
http://freedomdefined.org/Definition

[FSF] Free Software Foundation (FSF). *Free Software Definition*. 2013-06-18.
http://www.gnu.org/philosophy/free-sw.html

[OSI] Open Source Initiative (OSI). *Open Source Definition (Annotated)*. Version 1.9.
http://opensource.org/osd-annotated

[Wikimedia] Wikimedia Foundation. *Resolution: Licensing policy*. Passed 2007-03-23.
http://wikimediafoundation.org/wiki/Resolution:Licensing_policy

This work was conducted under contract N66001-11-C-0001, subcontract D6374-S5, Task GT-5-3329 for the Georgia Tech Research Institute and Department of Homeland Security (DHS). The publication of this IDA memorandum does not indicate endorsement by the Department of Defense or Department of Homeland Security, nor should the contents be construed as reflecting the official position of those Agencies. The material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-7013 (NOV 95).

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)
21-08-2013

2. REPORT TYPE
Non-Standard

3. DATES COVERED (From – To)

4. TITLE AND SUBTITLE
What is Open Security?

5a. CONTRACT NUMBER
N66001-11-C-0001, subcontract D6384-S5

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)
David A. Wheeler

5d. PROJECT NUMBER

5e. TASK NUMBER
GT-5-3329

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES
Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311-1882

8. PERFORMING ORGANIZATION REPORT NUMBER
NS D-4993
H 13-001186

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Joshua L. Davis
Georgia Tech Research Institute (GTRI), 250 14th Street NW, Room 256, Georgia Tech Research Institute (GTRI), 250 14th Street NW, Room 256, Atlanta, GA 30318

10. SPONSOR'S / MONITOR'S ACRONYM
GTRI

11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
Project Leader: David A. Wheeler

14. ABSTRACT

This document provides a definition of the term "open security," along with some background, clarifications, and discussion. Open security is the application of open source software (OSS) approaches to help solve cyber security problems. OSS approaches collaboratively develop and maintain intellectual works (including software and documentation) by enabling users to use them for any purpose, as well as study, create, change, and redistribute them (in whole or in part). Cyber security problems are a lack of security (confidentiality, integrity, and/or availability), or potential lack of security (a vulnerability), in computer systems and/or the networks they are a part of. In short, open security improves security through collaboration.

15. SUBJECT TERMS
Open source software, security, cyber security, collaboration, vulnerability, Open Source Definition, Free Software Definition, Definition of Free Cultural Works, software, hardware, documentation, open access, open data.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Joshua L. Davis
a. REPORT	b. ABSTRACT	c. THIS PAGE	Unlimited	8	19b. TELEPHONE NUMBER (Include Area Code) 678-831-0182
Unclassified	Unclassified	Unclassified			