

[WP-004]

Whitepaper: The Future of 'Open Source' and Information Security

An Opinionated Discussion Regarding 'Open Source' and Information Security

Version 040323

March 2004

Author: Bob Radvanovsky, rsradvan@unixworks.com

(A special thanks goes to those listed for being my "sounding board" on this project.)

Copyright © 2004 Bob Radvanovsky. All rights reserved.



Limited Liability Statement

In no event shall the author(s) be liable for any found errors contained herein or for any direct, indirect, special, incidental or consequential damages (including lost profit or lost data) whether based on warranty, contract, tort, or any other legal theory in connection with the furnishing, performance, or use of this material.

The information contained within this document may be subject to change without any notice. No trademark, copyright, or patent licenses are expressly or implicitly granted (herein) with this whitepaper.

Documentation pertaining to any security-related technical or proprietary information, its data and all information provided and contained within this document is considered proprietary in nature and subject to copyright protection and is intended solely for use by its owner. Additionally, this documentation is solely for the purpose of discussing the future of 'open source' and how it may (or will) impact information and/or network security, and is not dependent upon any specified architecture, hardware platform or software.

The name "LINUX" is a registered trademark of Linus Torvalds.

The name "UNIX" is a registered trademark of The Open Group. [ref: <http://www.opengroup.org/legal.htm#trademarks>]

The name "Windows" is a registered trademark of Microsoft Corporation.

The name "Apple" and "Apple Macintosh" are registered trademarks of Apple Computer, Inc.

All other product names mentioned herein are trademarks or registered trademarks of their respective owners. NOTE: Any names not outlined or mentioned above are fictional in nature; as such, any relation to any name or trademark (if any) is purely coincidental.

Introduction

One of the hottest topics right now is the (very) heated debate of whether or not to implement 'open source' / 'open system' solutions in a corporate environment. This would include both publicly and privately owned/operated corporate environments, not to mention government entities. The United States government has been a huge proponent of the 'open source' mindset for years, and is investigating any financial responsibilities associated with implementing solutions that are considered 'open source'.

Though the general public may not be aware of this, the Defense Advanced Research Project Agency's network (called "DARPA NET", later called "ARPA NET") was built using the UNIX operating system environment, which was, at the time, a privately funded project sponsored in part with AT&T / Bell Laboratories. The federal government embraced the implementation of the ARPA NET network for a more efficient communication system, esp. during times of national crisis, such as during a nuclear attack/bombardment. Over the years, much of the networking infrastructure of today that we call "The Internet" was based upon, founded by, and continues to use -- 'open source' and 'open system' architectures.

Although many people may not know it, but much of what is (now) taken granted for as key, critical network protocols on/across the Internet – is 'open source' and/or 'open system'.



Micro-sized?

Microsoft Corporation has felt threatened by the presence of 'open source' and 'open system' architectures. This may be that Microsoft's software environments are (by design) 'closed system' architectures. Lately, Santa Cruz Operations (aka "SCO") has fired several lawsuits against the 'open source' community, initially directed towards IBM Corporation, but now includes a plethora of varied companies, most of which develop, support and maintain the LINUX operating system and its environments. By its nature, LINUX is licensed as 'open source', under the GNU Public License (GPL).

The definition of 'closed source' versus 'open source' development has been debated for many years, but in a nutshell, the difference is how many architectures are available for that environment (can Microsoft Windows run natively under the Sun Microsystems architecture?), and community-like collaborative environments of shared knowledge and ideas that are community-owned, rather than corporate-owned. Some may argue that the Free Software Foundation (FSF), which has fronted the GPL licensing mechanism (and others similar to it), effectively "owns" all software and environmental products that are licensed under the GPL licensing umbrella.

Under the GPL licensing mechanism, FSF clearly states that⁵:

"When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. "

FSF makes it known that GPL is for protecting the rights of the software developers, not necessarily the corporations that may use it. This is may be what Microsoft (and others who support Microsoft, such as SCO) object to.

Recently, Microsoft Corporation has spearheaded and is part of an industry standard initiative called the "Trusted Computing Platform Architecture" (or "TCPA"). What this architecture claims and states is that it will (supposedly) provide a more robust and secure environment and architecture that will support trusted computing and communications in an un-trusted world⁷.

Though this paper is not meant to debate what is or is not 'open source'; rather, it raises several issues, esp. in the area of information and network security, and how TCPA will



impact both it and the future of 'open systems', and how both architectures will operate. The Electronic Frontier Foundation (EFF) has been a large advocator and promoter of civil rights and free speech avocation on, within and throughout the Internet. Their statement about attestation (that is, the restriction of ones digital right to reproduce, review, copy, or distribute data/information) fits perfectly into how security may play an even greater role of importance in the years ahead. But, darker times seem to loom future prospects as the requirements to comply with a trusted computing environment are further reinforced and pushed upon the masses and general public⁸. So what does this all mean?

The Computerized Society

Well – the future of both information/network security, as well as 'open source' will depend (largely) to how companies view 'open source': is it a threat to the mature corporate environmental stronghold, or will it be embraced openly? Right now, based upon the audiences that the information about the TCPA and it's parent organization, The Trusted Computing Group (TCG), displayed or discussed using an almost 'doublespeak'⁷ language (the term "doublespeak" was introduced by Orwell's novel, "1984", in which freedom of speech was prohibitive) about 'open source'. Strange thing is, is that I have observed that when corporate entities (which includes governments, too) starting speaking in riddles (as in 'doublespeak'), their intentions are hidden within normal spoken or written form, usually with a hidden message embedded within the message that is in plain form and clear text.

Society (as a whole) is showing an even greater dependence upon computerized gadgets, devices and handhelds. Computers are (pretty much) everywhere now, and are included in almost everything that we use on a daily basis. From watches, to automotive vehicles (cars), to vending machines, computers have been introduced to make life (supposedly) more efficient and easier for humanity. But what if the introduction of computers into everything was a grand, master scheme of further controlling the masses of humanity to be at the whim of a few, controlling people?

Not to sound off in a manner similar to the Tale of Chicken Little, but, when the Internet first came out, many "experts" stated that the Internet would bring about the end of humanity, and in fact, several movies capitalized on that very thought, such as the trilogy of movies referred to as "The Matrix". Many people know what this is all about, and it may be very, conceivably all possible. We (as humans) could invariably cause our own demise, ending human individuality and freedom (as we know it), thus becoming slaves to "The Machine". In some regards, we are already there in our ever-increasingly growing dependences upon machines to perform menial tasks. We now (as a society) have become lazy and complacent, and would rather have something (or someone) else *think* for us. Prime examples are how some of the more silly bills have been passed within the United States, into laws that are practically unenforceable (case in point -- the Anti-Spam Act, called the "CAN-SPAM Act of 2003", and resulting from its implementation, appears to have caused an even greater number of unsolicited electronic mailings to the masses since its inception⁹). Strangely enough though are even sillier bills/laws (not just the United States, this includes other countries, such as those within the European Union) that are coming our way.



Support Your Local 'Sheriff'

As many people are being made more aware of the intentions of mature, large corporate entities of what may happen with the implementation of the TCPA, being aware of the TCG's intentions does not entirely merit its rejection either. If at all, it demonstrates further need for security, both at home and at the workplace, but under the terms defined by the home-user or corporate-user using them. Having a trusted environment is not entirely a bad thing. If it all, it promotes "safer sex" with others; thus, it will have a beneficial measure to the welfare of the users.

Not all security mechanisms are bad. With the introduction of "Caller ID" (or "CID"), many thought that this was an invasion of their privacy, but in reality, it significantly reduced the number of unsolicited (and certainly unwanted) telephone calls from the telemarketing industry. Perhaps TCPA will provide a role similar to that of CID.

How will information and network security play in the future?

Undoubtedly, security will play an even greater role in the future, but not as what many think. Security will play the role of 'enforcer' and 'enabler', depending upon the circumstances, and will allow or restrict access based upon mandated access control rules and lists (very similarly to those that first came out for the United States military in the early 1970's). Policy management, forensics management, legal enforcement will all play a crucial role in the future.

The Future of the Internet

As you read this document, there is another "Internet" which presently exists. Dubbed "*Internet Version 2.0*", this is used for dedicated, advanced research in theoretical physics and dynamics¹⁰. So far, only a few select locations have unrestrictive access to network communication speeds that are upwards (if they have not surpassed this statistic already) of (aggregately) 200 Gbit/sec (4 x 40 Gbit/sec 'dark fiber' pipes). This speed is required for 'grid computing technology'¹¹, which requires security of a similar nature to that of TCPA. In this case, 'grid computing' allows end-users to access a portal, which in turn, accesses a client-server that provides the front-end communications to the backend servers, which comprise of the computing capabilities. The storage capabilities are part of another group at a distantly remote location, and the displaying capabilities are yet part of another group at another distantly remote location. So you can now see why the extremely huge bandwidth is required.

In some regards, TCPA may very well be Microsoft's implementation of a 'grid' environment. Everyone will "see" everyone else in a secured fashion. Is this utopic? You bet! If at all, this is only allowing a greater number of parties/entities a greater or unfettered/unbridled access to *your* data – whether this may be within the corporate environment, or your own home workstation, if you are "connected" to the Microsoft 'grid', everyone will be able to access your data "on demand". So... Security will play an even greater role in ensuring that people stay where they are supposed to be, and nowhere else.



The Future of Information Security

As a whole, our society is becoming increasingly more 'compartmentalized' (also have heard the term "silo", as in "grain silo"), thus corporations want to ensure that data and information get to their proper destination. In some regards, there were several various paragraphs stating that TCPA could be used to the corporations' benefit, esp. for corporate scandals that not only of an unethical nature, but illegal, too (think Enron and Worldcom). Though I am uncertain where this will play with information security of the future, this may be one of those gray areas that may be managed by government entanglements rather than corporations.

As the United States further implements preventative security measures through the Department of Homeland Security (DHS), DHS may very well have an even greater role in how the corporations would be managed (go to previous paragraph about imperial entanglement). If the corporations are going to require users to compliancy issues (meaning that TCPA is inevitable, not avoidable), then "who watches the watchers"? Obviously, governments (in of themselves) are considered "corporate entities", and they are the watchers who watch the other watchers (say this three times faster while twirling around as fast as you can). Thus, within the United States, DHS may require security/compliancy officers at each location for the larger corporations, and/or provide their own compliancy officers for the small or medium-sized businesses that cannot afford to have a dedicated compliancy officer. What this translates to is nothing shy of the "political officer" that existed during the days of the 'Cold War' between the United States and the (former) Soviet Union.

Would DHS require compliancy? Obviously, if the federal government is getting ready to embrace 'open source', and the computer technology industry is quickly merging efforts to provide "securified" environments, then someone (or something) will need to regulate all of this. Similar to the Department of Precrime from the movie "Minority Report", the federal government will require some level of compliancy. This is the direction that information and network security are heading.



Bibliography

1. ref: http://www.circleid.com/article/337_0_1_0_C/
The Internet Infrastructure: Stability vs. Innovation, October 22, 2003, Kevin Werbach.
2. ref: <http://www.mids.org/mn/806/dns.html>
The U.S. DNS White Paper, John S. Quarterman.
3. ref: <http://www.netaction.org/opensrc/future/oss-whole.html>
The Origins and Future of Open Source, Nathan Newman
4. ref: http://www.atis.org/tg2k/open_systems_architecture.html
open systems architecture.
5. ref: <http://www.fsf.org/copyleft/gpl.html>
GNU General Public License.
6. ref: http://www.cypherpunks.to/TCPA_DEFCON_10.pdf
7. ref: https://www.trustedcomputinggroup.org/downloads/TCG_Backgrounder.pdf
8. ref: http://www.eff.org/Infra/trusted_computing/20031001_tc.php
9. ref: <http://www.eweek.com/article2/0,1759,1551150,00.asp?kc=EWNWS031904DTX1K0000599>
Survey: Spam Erodes U.S. Trust in E-Mail, March 18, 2004, Anick Jesdanun.
10. ref: <http://www.teragrid.org/>
11. ref: <http://www.gridcomputing.org/> and ref: <http://www.gridbus.org/grid2004/>

