The Big Challenge:
Building Trust while favouring Openness

2nd ENISA International Conference on Cyber Crisis Cooperation and Exercises

Athens, September 23, 2013

Luigi Romano
luigi.romano@uniparthenope.it

Fault and Intrusion Tolerant NEtworked SystemS

Excerpts from ENISA study recommendations [1]

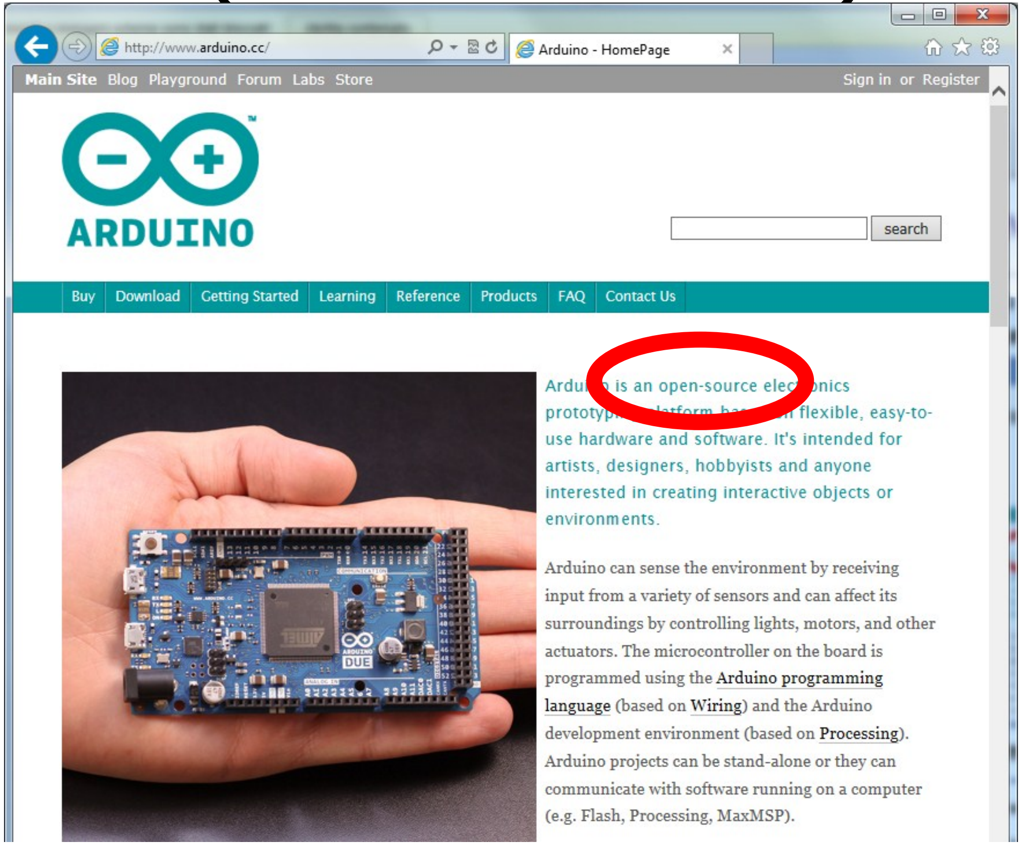
- Recommendation 1: **Improved and innovative trust models.** Currently, most commercial systems operate with implicit trust from their operators only … These **trust models need to be augmented to enable end-to-end verifiable trustworthiness** of ICT systems …
- Recommendation 3: **Deeper study of good practices currently used in** various **industry** segments and in **government** procurement. Good practices in supply chain management, which are already deployed by the industry …
- Recommendation 7: … There is an opportunity for **industry and academia** to study balanced approaches for addressing policy needs in the area of **ICT supply chains on a global scale**, based on the **examples of good practices** available **from** a range of **use cases** …

Objectives of this talk

- Present a (purposely) un-balanced analysis of pros and cons of the Open Source and Closed Source software development models (and related Supply Chain)
- Provide evidence that there is a strong business case for Open Source Software (OSS) adoption, and thus an equally strong motivation for chasing Supply Chain Integrity (SCI) trust models that are rigorous, while still favour openness
- Stimulate discussion, in an attempt to define a strategy for effective research, to be done jointly by industry and academia, towards the development of such improved trust models
- Make proposals for immediate action points to extend the network of experimenters willing to participate in the ENISA Cyber Exercises upcoming campaign on SCI integrity

Side Note

Focus of talk is on software,
but claims also hold (with minor differences) for hardware …

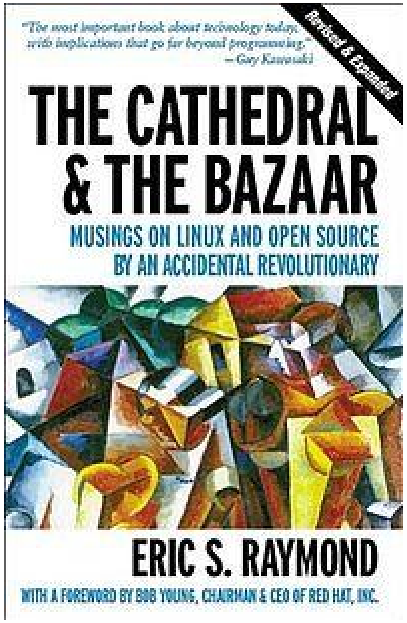


Arduino is an open-source electronics prototyping platform based on flexible, easy-to-use hardware and software. It's intended for artists, designers, hobbyists and anyone interested in creating interactive objects or environments.

Arduino can sense the environment by receiving input from a variety of sensors and can affect its surroundings by controlling lights, motors, and other actuators. The microcontroller on the board is programmed using the Arduino programming language (based on Wiring) and the Arduino development environment (based on Processing). Arduino projects can be stand-alone or they can communicate with software running on a computer (e.g. Flash, Processing, MaxMSP).

… and it will be even more so in the future

Two alternative approaches


"The most important book about technology today, with implications that go far beyond programming." —Guy Kawasaki
Revised & Expanded
THE CATHEDRAL & THE BAZAAR
MUSINGS ON LINUX AND OPEN SOURCE BY AN ACCIDENTAL REVOLUTIONARY
ERIC S. RAYMOND
WITH A FOREWORD BY BOB YOUNG, CHAIRMAN & CEO OF RED HAT, INC.

Closed Source:

1. Quality assurance
2. Quality control

Open Source [2]:

1. "Release early and release often"
2. "Given enough eyeballs all bugs are shallow"

Closed Source vs Open Source [3] [11]

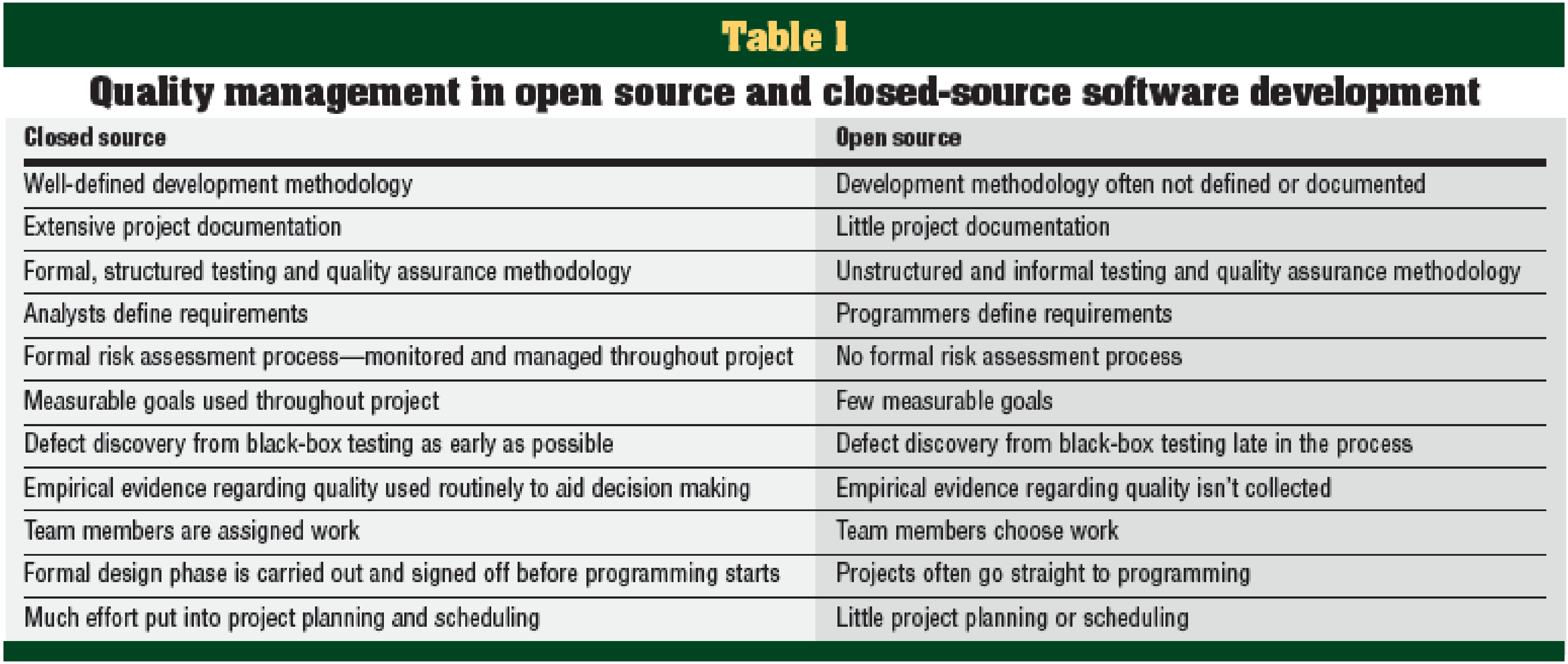


Table 1

Quality management in open source and closed-source software development

Closed source	Open source
Well-defined development methodology	Development methodology often not defined or documented
Extensive project documentation	Little project documentation
Formal, structured testing and quality assurance methodology	Unstructured and informal testing and quality assurance methodology
Analysts define requirements	Programmers define requirements
Formal risk assessment process—monitored and managed throughout project	No formal risk assessment process
Measurable goals used throughout project	Few measurable goals
Defect discovery from black-box testing as early as possible	Defect discovery from black-box testing late in the process
Empirical evidence regarding quality used routinely to aid decision making	Empirical evidence regarding quality isn't collected
Team members are assigned work	Team members choose work
Formal design phase is carried out and signed off before programming starts	Projects often go straight to programming
Much effort put into project planning and scheduling	Little project planning or scheduling

- **Less confusion for customers**
- **Unified experience**
- **More profitable**

- **Larger Developer Support**
- **Customizable**
- **Extended Community Support**

Open Source model: not so bad after all

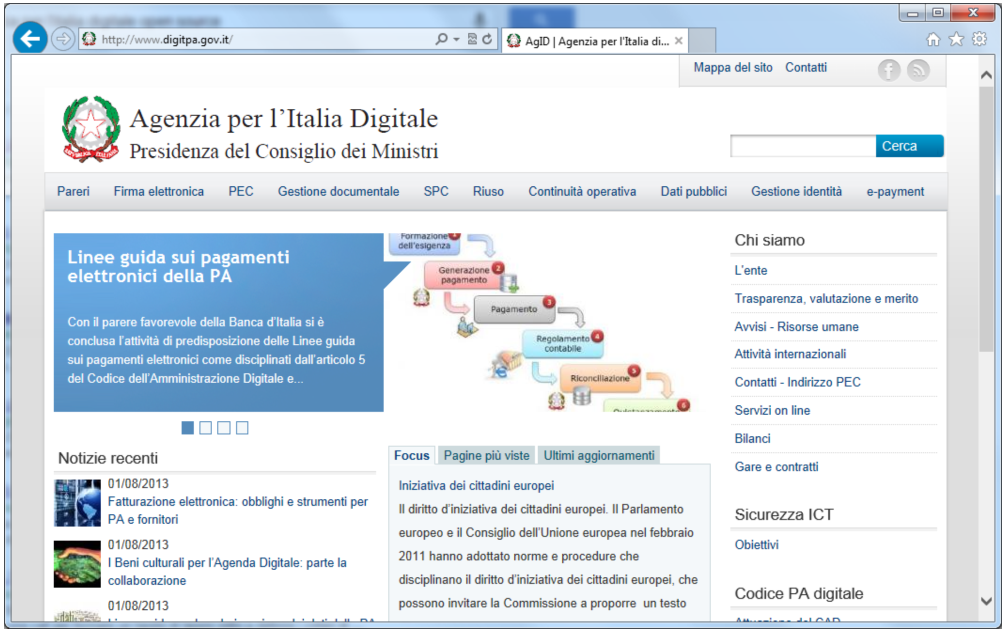
“Every good work of software starts by scratching a developer's personal itch” [11]

- Success stories from **direct experience**:
  - Linux, Apache, Mozilla, Perl, OpenOffice, …

- **Experimental evidence** of success stories:
  - Quality of 100 applications developed for Linux, measured using a commercial software measurement tool [4]
  - They found that the quality of code produced by open source is in most cases comparable to what is expected by an industrial standard [4] (or even better than that [12])

Open Source in the Public Administration

- The diffusion of OSS is constantly growing in the Public European scenario [6]
- **“Nearly half of European local government bodies are using open source software while nearly a third don't know that they are using open source at all ” [7]**
- Public Administration authorities , in many countries, are actively promoting the adoption of OSS solutions [8]



Linee guida sui pagamenti elettronici della PA

Con il parere favorevole della Banca d’Italia si è conclusa l’attività di predisposizione delle Linee guida sui pagamenti elettronici come disciplinati dall’articolo 5 del Codice dell’Amministrazione Digitale e...

Notizie recenti

01/08/2013
Fatturazione elettronica: obblighi e strumenti per PA e fornitori

01/08/2013
I Beni culturali per l’Agenda Digitale: parte la collaborazione

01/08/2013

Iniziativa dei cittadini europei

Il diritto d’iniziativa dei cittadini europei. Il Parlamento europeo e il Consiglio dell’Unione europea nel febbraio 2011 hanno adottato norme e procedure che disciplinano il diritto d’iniziativa dei cittadini europei, che possono invitare la Commissione a proporre un testo

Main Messages

- People trust Open Source
- People trust Open Source **despite the absence of a** (well defined) **trust model in the Open Source supply chain**
- Surprisingly enough, combined expertise of an unlimited number of programmers and users results in an un-structured yet trustworthy Supply Chain, whose integrity level is comparable to the one achieved by the traditional closed model
- Additionally, Quality is receiving more and more attention in the Open Source community [5]
- **All in all, Open Source Software (OSS) principles are a value that we cannot throw away**

Proposal for Cyber Exercises on SCI integrity

- Cooperative research – to be done jointly by industry and academia – aiming at developing SCI trust models that are:
  - Rigorous enough to guarantee quality
  - Flexible enough to accommodate openness
- Issues that should be addressed (non exhaustive list):
  - Implementing integrity assessment mechanisms for all phases of the product lifetime (including operation) → this implies support for dynamic assessment techniques
  - Ability of attracting volunteer programmers, and having them coexist with paid programmers
  - Encouraging innovation and creativity, while retaining control of the overall process
  - Handling deadlines, while respecting freedom and self-organization

Expression of Interest in Cyber Exercises - SERIT

- SERIT (Security Research in ITaly) is the technological platform for national security jointly promoted by the National Research Council (CNR) and Finmeccanica [9]
- It currently includes 250+ companies and research institutions involved in security research
- SERIT is willing to participate in the Cyber Exercises that will be organised by ENISA on the subject of Supply Chain Integrity

- **SERIT contacts for this activity:**
  - Platform Co-chairs: **Cristina Leone** and **Fabio Martinelli**
  - Cyber Security Chair: **Luigi Romano**

Expression of Interest in Cyber Exercises - MASSIF

- **MASSIF** (**MA**nagement of **S**ecurity information and events in **S**ervice **I**n**F**rastructures), FP7-ICT-2009-5 (ICT-2009.1.4 (b): Trustworthy Service Infrastructures)
- MASSIF has developed an advanced Security Information and Event Management (SIEM) solution (more info at: http://www.massif-project.eu/)
- MASSIF partner CINI is willing to make MASSIF Generic Event Translation (GET) framework and MASSIF Resilient Event Storage (RES) facility available for the experiments
- **MASSIF Contact for this activity:**
  - CINI PI: **Luigi Romano**

Expression of Interest in Cyber Exercises - SAWSOC

- **SAWSOC** (**S**ituation **AW**are **S**ecurity **O**perations **C**enter) - Starting: November 1, 2013
- FP7 – SEC 2012 (Topic SEC-2012.2.5-1 Convergence of physical and cyber security – Capability Project)
- SAWSOC aims at bringing a significant advancement in the **convergence** of physical and logical security
  - **Convergence:** effective cooperation (i.e. a coordinated and results-oriented effort to work together) among previously disjointed functions

- SAWSOC is willing to contribute to the Cyber Exercises
- **SAWSOC Contact for this activity:**
  - SAWSOC Technical Coordinator: **Luigi Romano**

References and pointers to additional info – 1/2

[1] “Supply Chain Integrity - An overview of the ICT supply chain risks and challenges, and vision for the way forward”, ENISA, 2012

[2] book : http://shop.oreilly.com/product/9780596001087.do

[3] Aberdour, M. "Achieving Quality in Open Source Software“, IEEE Software, vol. 24, no. 1, pp. 58-64, January/February, 2007

[4] L. Angelis et al., “Code Quality Analysis in Open Source Software Development”,C Information Systems J., vol. 12, no. 1, 2002, pp. 43–60

[5] http://www.opensourcetesting.org/

[6] European Commission (EC). (2006). i2010 eGovernment Action Plan:Accelerating eGovernment in Europe for the Benefit of All, -COM(2006)173 Final Report, retrieved 3 February 2009 from http://ec.europa.eu/information_society/newsroom/cf/itemshortdetail.cfm?item_id=3140

References and pointers to additional info – 2/2

[7] The Register. Open Source Taking Over in Europe, available at: http://www.theregister.co.uk/2005/10/21/opensource_government

[8] “Linee guida per l’inserimento ed il riuso di programmi informatici o parti di essi pubblicati nella “banca dati dei programmi informatici riutilizzabili” di digitpa”, available at: http://www.digitpa.gov.it/riuso-del-software

[9] SERIT platform Web Site, http://www.piattaformaserit.it/

[10] MASSIF project Web Site, http://www.massif-project.eu/

[11] http://info.nsiserv.com/network-support-computer-services-CT/bid/29956/Comparison-between-open-source-and-closed-source-software

[12] http://www.coverity.com/company/press-releases/read/annual-coverity-scan-report-finds-open-source-and-proprietary-software-quality-better-than-industry-average-for-second-consecutive-year

Contact Info

Luigi Romano
luigi.romano@uniparthenope.it
prof.luigi.romano@gmail.com
Cell: +39-333-3016817
Tel: +39-081-5476700

The **F**ault and **I**ntrusion **T**olerant **NE**tworked **S**ystem**S**
(FITNESS) Research Group
http://www.dit.uniparthenope.it/FITNESS/