Inside Risks: Evaluation of Voting Systems

from Communications of the ACM Volume 47, Number 11 (2004), Page 144

P.L. Vora, B. Adida, R. Bucholz, D. Chaum, D.L. Dill, D. Jefferson, D.W. Jones, W. Lattin, A.D. Rubin, M.I. Shamos, M. Yung

The recent spate of security issues and allegations of "lost votes" in the U.S. demonstrates the inadequacy of the standards used to evaluate our election systems. The current standards (the FEC Voting Systems Standards) along with the revision being developed by IEEE 1583 (see the article by Deutsch and Berger in last month's *Communications*) are poor from another perspective: they establish a single pass/fail threshold for all systems, thereby eliminating incentives for existing suppliers to improve their products and rendering the market unattractive to new entrants. Moreover, they fail to precisely define the properties that should be required of a voting system. Instead, the standards rely on specific designs that are more than 15 years old. These legacy designs handicap promising new approaches, such as the various voter-verified printing schemes. New systems are unnecessarily burdened, while their substantial advantages go unrecognized.

A set of well-defined properties would encourage the development and commercialization of better voting systems, especially when combined with objective ways to measure performance with respect to those properties. The overall result would then resemble the quantitative federal ratings for automobiles, where features such as vehicle safety and fuel efficiency form a basis for *Consumer Reports*-style comparative tables. Similarly, specific performance rating guidelines for different aspects of voting systems would provide meaningful metrics upon which system developers could compete. Decision makers, both regulatory and purchasing, would then be free to establish their own minimums for these metrics. Such a rating system can thus cleanly disentangle the development of the technical evaluation process from the various political and regulatory processes.

The Chair of the U.S. Federal Election Assistance Commission (EAC), DeForest B. Soaries, Jr., recently asked the technical community for assistance in determining a new standard. This community is no stranger to the area of voting system properties and standards: a number of authors have tried to characterize requirements, and, in 2002, the Workshop on Election Standards and Technology addressed similar issues. The performance properties for voting systems might include the following: integrity of the votes (both voter verification, "I can check that my vote was captured correctly" and public verification, "anyone can check that all recorded votes were counted correctly"); ballot secrecy (both voter privacy and resistance to vote selling and coercion); robustness (including resistance to denial of service attacks); usability and accuracy (including access for the disabled); and transparency (both of mechanism and election data).

The inherent differences in system architectures can be characterized abstractly on two levels. Architectures are first compared by how well each can satisfy the overall properties, then are characterized by the kinds of building blocks they need and by the assumptions they need to make about those blocks. A standard should provide an objective way to measure, for a particular actual system implementation, how well its building block instances ensure the properties required of them by the architecture of that system.

Suitable performance evaluation and measurement standards already exist for several types of building blocks: FCC 47CFR shielding and emissions, FIPS rating of tamper-resistant equipment, and the Common Criteria for software. For some properties, objective and repeatable measures of overall performance can be defined. For example, the accuracy of a user interface in capturing voter intent can be experimentally tested in a practical and repeatable manner, with the result expressed as an error rate. "Tiger team" and code review security evaluation (while certainly not foolproof) should play a role along with ordinary reliability testing. Ideally, this process of developing the properties and characterizing architectures would be exceptionally transparent, such as that for Internet RFCs, and would be subject to appropriate peer review. The refinement and adaptation of the measurement techniques would proceed as an ongoing parallel activity.

The EAC's request for assistance is a unique chance to positively affect the quality of our election systems, by tackling this new scientific and technical challenge and building a solid foundation. The aim should be to impact the 2006 elections, though the timing is already tight: the EAC is required to present technical recommendations to the House Administration Committee in April 2005. The technical community is faced with a significant need, a rare opportunity, and a growing urgency for coordinated technical effort in this area. (See www.vspr.org for further details.)

Free Software is Not Zero Cost

Ron Morrissey, GBC ACM memmber

Many people who are unfamiliar with free and open-source software practices are surprised to find that people are paid to write free software. The terms "free" and "open-source" tend to conjure images of long haired hippies writing code in their basements in a caffeine induced frenzy. There is a grain of truth in that stereotype, but, more and more often, businesses are paying their programmers specifically to work on projects which directly develop and extend free software.

The concept of being paid to write free software is not a new one. In truth, the Free Software Foundation (www.fsf.org) encourages people to charge as much as they wish or can for their efforts1. Richard Stallman, generally acknowledged as the father of free software, made a fairly comfortable living performing custom extensions to his earlier work for customers who needed extra functionality. The extensions were then made available for free to whomever wished to download them. Richard Stallman himself is currently compensated by a fellowship, but others have followed in his footsteps.

Linus Torvalds, the originator of the Linux operating system, is currently employed by the chip vendor Transmeta. Many of his duties involve ensuring that Linux runs correctly on the Transmeta processor line. Many of the Linux kernel maintainers are employed by companies which have a stake in Linux development, such as IBM and Red Hat. Again, enhancements to the Linux kernel are provided back to the community, and are available for free download.

There are several reasons that companies are willing to devote resources to developing "free" software. One reason has to a large extent to do with the fact that many companies rely extensively on custom or semi-custom software to manage the day-to-day functioning of their business. Extensions to commercial off-the-shelf packages are available in many cases, but interfacing to commercial products becomes difficult when source code is not available. This often leaves developers with no choice but to attempt to reverse engineer the commercial product in order to figure out how to effectively implement a needed extension. In other cases, extensions must be pasted on by saving a file from the commercial application, and then feeding the file into a program intended to process the data in the file and return custom data products (this may also require reverse engineering to figure out the file format).

Enter "open source" software. This software is distributed with the source code provided. The cost of the base software package is either zero or nominal depending on the distribution method. Since the source code is available, it is relatively straightforward (if not simple) to add desired functionality. The cost of customizing software for the task at hand is therefore lower if an existing open-source package is available, than to attempt customization of a proprietary software package

A second reason has to do with licensing costs. Since "open-source" software may be distributed free of charge, it can be considerably cheaper to provide with a system when a large number of units are involved than proprietary software.

Finally, there is time to market. For makers of embedded devices such as cable routers or FAX machines, a large body of existing code may be leveraged to decrease time to market considerably over starting from scratch, even with the aid of proprietary special purpose embedded operating systems (reason number 2 also comes into play here, as large numbers of devices are typically produced).

One thing that should be noted about this development model is that software is often not the end product for these businesses. Rather it is a means to an end, whether that end is data management in a call center or FAX machines. From the point of view of businesses such as this, the lowest cost way to manage their business is the key parameter in deciding what software model is used. If a proprietary software package is available that solves all their needs at a reasonable cost, then business will go that route. If custom software is required, then open-source becomes extremely attractive, as having the source makes it simpler for a hired consultant to modify the software. Since the companies core business is not software, sharing source code is a cost savings, not a restriction. Even firms such as IBM and Red Hat fit into this model. IBM sells hardware and software consulting services, both of which are enhanced by an open source development model. Red Hat distributes Linux for a fee, as well as providing software maintenance. For both distribution and maintenance products, Red Hats bottom line is enhanced by a more effective Linux product.

1 "Selling free software", www.fsf.org

Brain Teasers
(From Raytheon's Waiting Activities during Principles of Systems Engineering Course)

PAID I'M WORKED	San Francisco pane	DON'T DO IT	JUST*144*ICE
pay pay	A M **TOWN** N	KJUSTK	CAST CAST CAST CAST
TOR TOE	***gettingitall***	G W N E I D D	ERIF

1. I'm underpaid and overworked
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____
11. _____
12. _____

(annswers available in a future issue)

December Meetings

IEEE Consultants Network
Joint meeting with the Boston Entrepreneurs' Network

Topic: What Investors Really Want to See in Your Business Plan
Speaker: TBD
Date/Time: Tuesday, December 7, 7 PM
Location: Sheraton Lexington Inn, Lexington, MA
Details: http://www.boston-consult.org
Fee: $7.00 at door for non-members

Check the website for details

Boston University Corporate Education Free Seminar

Topic: Project Management
Date/Time: Monday, December 13, 6-9 PM
Location: BU Corporate Ed Center, Tyngsboro, MA
Details: http://www.butrain.com/misc/z100.asp?dept=360#707

Attend this FREE class, and experience for yourself Boston University's project management training. Gain a greater understanding of the recent trends in project management, why project management is so popular, and the benefits and requirements of PMP Certification. This session will be taught by one of our more than 50 PMP certified expert instructors who will lead you in discussion and engage you in an exercise to rate your organization's project management readiness.

Boston SPIN

Topic: Metrics
Speaker: Dr. Howard A. Rubin
Date: Tuesday, December 14, 6 PM Networking, 7:10 PM Presentation
Location: The Mitre Corporation, S Building, Bedford, MA
Details: http://www.boston-spin.org/meeting.html

Dr. Rubin possesses a Ph.D. from the City University of New York, which was awarded in the areas of Biology (Ecology/ Oceanography) and Computer Science. Dr. Rubin is internationally recognized for his work academically and commercially as an author, researcher, talented speaker, and consultant in the areas of IT measurement, techno-business strategy, global software economics, the workforce of the future, the business value of technology, and performance measurement/benchmarking.

Dr. Howard A. Rubin is a Professor Emeritus of Computer Science at Hunter College of the City University of New York, a Board member, Chief Strategy Officer, and Executive Vice President of META Group, Inc., and a former Nolan Norton Research Fellow. In the spring of 2000, he was appointed to the White House's private sector e-commerce Working Group in support of G-8 activities. In addition, because of his extensive work in worldwide technology data collection and benchmarking, Dr. Rubin has been a member of the Global Information Economy (GIE) Working Group of the State Department's Advisory Committee on International Economic Policy (ACIEP).

Through his product experience and research, Dr. Rubin has collected data and organized it into what may well be the world's largest information technology benchmarking and trend tracking IT and business database - drawing on data gathered through a network of more than 30,000 professionals in about 10,000 companies covering 50 countries. (www.metricnet.com).

***Real Times* Editor**
Rochelle Goren, rochelle_goren@comcast.net

GBC/ACM Officers (2004 - 2005)

President
Peter Carmichael, pcarmichael@alum.mit.edu

Vice President
Jay Conne, conne@acm.org

Secretary
Ed Bristol, e.bristol@comcast.net

Treasurer
Yona Carmichael, treasurer@gbcacm.org

Past President
Stephanie Collins, jsmco@attglobal.net

Local Special Interest Group Chairs

GB/SIGCHI
Gabriel Spitz, spitz@aptima.com

SIGGRAPH/Boston
Samuel Murphy, samuelmurphy@gmail.com

GB/WEB TECH
Dan Jacobs, (781) 273-5825, daniel.jacobs@acm.org

Standing Committee Chairs

PDS Committee
Peter Barzdines, (617) 924-4072 (home), peterbar@world.std.com

Program Committee
Peter Mager, p.mager@computer.org

Interest Group Committee
Sam Cardman,sc@mbunix.mitre.org

Acting Membership Chairman
Kenneth Baclawski, kenb@ccs.neu.edu

Volunteer Coordinator
Glenn Hoffman GlennHoffman@mac.com

Webmaster
Michael Ciaraldi, ciaraldi@ciaraldi.com, *http://www.gbcacm.org*

The Real Times is published ten times per year (September through June) and is the official newsletter of the Greater Boston Chapter of the Association for Computing Machinery, First-class postage paid at Boston, MA, 02101.

Timely notices of events, meetings, and other activities of interest to the Chapter's Membership should be submitted by the 10th of the month Before the intended issue and sent, with attention to the Managing Editor to:

GBC/ACM, P.O. Box 465, Lexington, MA 02420
(781) 862-1181

The Chapter's mailing list is available to related professional organizations or for commercial use. Please contact the Membership Chair at the address above when requesting mailing lists.

Annual subscription cost is included in the Chapter Membership dues of $10.00. See top line on mailing label for membership expiration date. Library subscriptions are free. Please send orders for copies to the Chapter mailing address above.

We would like to thank our PDS Sponsors for their support:

Softpro
75 Third Ave., Waltham; 197G Post Rd West, Marlboro
http://www.softpro.com

Quantumbooks
Corner of Ames & Broadway, Cambridge
http://www.quantumbooks.com

PCs for Everyone
24 Charles Street, Cambridge, MA 02141
http://www.pcsforeveryone.com

Websites of some Local Groups

GBC/ACM
www.gbcacm.org

SIGGRAPH
www.siggraph.org/chapters/boston

Boston SIGCHI
www.gbsigchi.org

WebTech
www.acm.org/chapters/webtech

SPIN
www.boston-spin.org

IEEE
www.ieeeboston.org

IEEE Consultants Network
www.boston-consult.org

Boston-area User Group Calendar
www.bugc.org

January, 2005 Meetings
Greater Boston SIGCHI

Topic: So, What Do You Do?
Speaker: Ilise Benun
Date/Time: Tuesday, January 11, 2005 6:30 PM - Refreshments, 7 PM - Meeting
Location: Sun Microsystems, Burlington, MA
Details: http://www.gbsigchi.org/mtg.html

How do you answer that question? Do you say something that engages or confuses your listener? Do they understand or do their eyes glaze over? Do you vary your answer depending on your listener and what they might understand? If this is an issue for you at all, then this workshop is for you.

To kick off the New Year, make a resolution to come up with something coherent and clear. How? Attend this workshop with Ilise Benun, author of "Self Promotion Online," who will lead an interactive session during which you will create 15 and 25-word blurbs that you will be able to use immediately in a wide variety of situations.

Ilise Benun is a nationally recognized expert on self promotion and marketing, and VP of the NYC chapter of UPA. She is the author of Self Promotion Online and Designing Web Sites for Every Audience and has conducted seminars and workshops on self promotion for UPA, Graphic Artists Guild, Women in Communications, American Marketing Association, and City University of New York, among others. Through her Marketing Mentor program, Benun also works one-on-one with clients to teach them how to promote their services.

****

Greater Boston Chapter of ACM Spring 2005 Professional Development Series

Look for our announcements

Are you a current member of GBC/ACM?*

If not, join! The $10 annual membership fee offers many opportunities for development, through regular and engaging interaction with local contemporaries in addition to access to our popular PDS seminars. Mail in your membership form today!

Name: _____

Address: _____

City/State/Zip: _____

Phone Number: _____

Please make checks payable to GBC/ACM and mail to:
P.O. Box 465
Lexington, MA 02420

(*Check your address label for expiration date.)

*** December Calendar of Events ***

Date of Event	Page	Sponsor	Location
December 7	3	IEEE Consultants Network	Sheraton Lexington Inn, Lexington, MA
December 13	3	BU Corporate Training	BU Corporate Center, Tyngsboro, MA
December 14	3	Boston SPIN	Mitre, S Building, Bedford, MA
December 16	1	GBC/ACM	MIT E51-315, Cambridge, MA

If the top line of your mailing label below reads **EXPIRED, please renew your membership (for just $10/yr). For that $10 you get a copy of this newsletter/local event calendar mailed to any address you choose plus the right to attend PDS seminars at the member rate. Please consider renewing for more than one year at time. Your support helps make possible the wide array of GBC/ACM activities.**

The Official Newsletter of the Greater Boston Chapter of the acm

The Real Times

Vol. 44 No. 4 www.gbcacm.org December 2004

GBC/ACM December 2004 Meeting

Topic: C# Generics vs. C++ Templates
Speaker: Richard Hale Shaw, Richard Hale Shaw Group
Date/Time: Thursday, December 16, 2004, 7:00 PM
Location: MIT Room E51-315

The 2005 release of the .NET Framework - and the C# language - will proffer a feature of great interest to C++ developers who're interested in .NET: Generics. Generics - like C++ templates - let you create types or methods that are - in one or more respects - typeless when defined, but available to be strongly typed when used and consumed. Unlike C++ templates, however, Generics are not a facet of a programming language like C++ (or C#), but instead are a product of the .NET Common Language Runtime (CLR). How do Generics differ from C++ templates? Can they be used to solve the same problems - or not? And, will the appearance of Generics mean that .NET will follow with a STL-like library for C# (and VB.NET) developers to use? In this session, we'll look at Generics: what they are, how they work, and what you can do with them. We'll also look at the .NET model for generic type instantiation, and compare it to template instantiation in C++. And we'll compare and contrast these similar - but fundamentally different - models for creating parameterized types, as well as the implications of Generics on .NET Reflection and Metadata, Collections and Remoting.

Richard Hale Shaw is a Microsoft MVP for C#, and a consultant and lecturer who focuses on Managed Code development of distributed systems with the C# Language and the .NET Framework. He's a frequent INETA speaker (www.ineta.org), Chair of C# Live (www.vslive.com), and the CEO of the Richard Hale Shaw Group (www.RichardHaleShawGroup.com). Richard taught himself to program in C (and later, C++) in 1982, and began writing and speaking on contemporary software development topics as a contributing editor to PC Magazine and Microsoft Systems Journal (now MSDN Magazine) in 1988. He's consulted to thousands of developers on C++, MFC, COM, ATL, .NET and C#, and authored the .NET BootCamp (a 5-day hands-on course), the .NET Patterns & Practices BootCamp, and the Advanced .NET BootCamp. Over the years, Richard has created and organized a number of developer events (e.g., the Visual C++ Conference).

E51 is the Tang Center at 70 Memorial Drive. It is at the corner of Wadsworth St. between Memorial Drive and Amherst St., directly across Wadsworth St. from the Faculty Club and main building of the Sloan School. You can go to <www.mit.edu> and click on "map" to see visually where this is. The talk is in room E51-315.

The Greater Boston Chapter of the
P.O. Box 465
Lexington, MA 02420

GBC/ACM is a non-profit educational and scientific society.
(781) 862-1181 - www.gbcacm.org

First Class:
Dated Materials

Address Service Requested

First Class
Presorted
U.S. Postage
PAID
Boston, MA
Permit Number
55536