


Date of event	Page	Sponsor	Location
May 1	5	GBC/ACM	MT
May 5		SIGGRAPH	
May 20	1	GBC/ACM	BBN/GTE, Cambridge
May 26	3	IEEE/CN	ADL, Cambridge
May 27	4	IEEE/CS	Marcam, Newton

If the top line of your mailing label below reads ****EXPIRED****, please renew your membership at the very affordable rate of \$10/yr. Please consider renewing for more than one year at time. It saves all of us some labor. For that \$10 you get your very own copy of this newsletter/local event calendar. Thank you.



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

First Class
 Presorted
 U.S. Postage
PAID
 Boston, MA
 Permit Number
 56536

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

First Class:
Dated Materials





The Real Times

Vol.38 No.5

www.acm.org/chapters/gbc

May 1999

GBC/ACM Monthly Meeting

The Mao Zedong Approach to Public Key Infrastructures

Dr. Stephen T. Kent

Chief Scientist- Information Security, BBN Technologies

Director, Security Practice Center, GTE Internetworking

Chief Technical Officer, CyberTrust

Thursday, May 20, 7 pm

Refreshments at 6:30 pm

BBN/GTE Newman Auditorium, 10 Fawcett St, Cambridge, MA.

Some popular models of public key infrastructure (PKI) embody a notion that only a few certificates will be issued to each user to represent that user in interactions with many different applications (services). Generic, public CAs like those operated by VeriSign adopt this notion. However, operating a public CA service of this sort requires balancing liability concerns, acceptable cost models, levels of authentication assurance, and name space issues. It is not clear that this model scales well or that it does a good job of addressing the needs of both subscribers and relying parties.

Another approach to PKIs is motivated by the observation that individuals have many existing relationships with various organizations. This approach leverages the existing databases maintained by organizations to track employees, customers, members, etc. Certificates issued by organizations not for general use, but focused on a specific application context, avoid many of the problems facing generic, public CAs. For example, liability can be well understood because the certificate is bounded in its use. The level of assurance for authentication is determined solely by the issuer, in the context of the application, and the issuer's database provides data associated with the subject that may be used to support on-line registration with fairly high levels of assurance. Naming problems disappear because each subject is already assigned a unique name in the issuer's database.

Continuation and Speaker Biography on page 3

Directions to Bolt Beranek and Newman (BBN)/Recorded directions: (617) 873-4567

From Route 128, Lexington: Take Route 2 inbound. The four-lane highway narrows to two lanes near Route 16. At the traffic light bear right onto Alewife Brook Parkway. Proceed past shopping centers to the Fresh Pond Rotary. Take the first right onto Concord Avenue. Fawcett Street is one block down Concord Avenue, on the right.

From the Mass. Pike: Take the Pike inbound to the Cambridge/Allston exit. Exit onto the Cambridge off-ramp and take Cambridge Street. Turn left onto either Storrow or Memorial Drive. (Storrow Drive is on the Boston side of the Charles River and Memorial Drive.)

From Storrow and Memorial Drives: Take Storrow or Memorial Drive west: follow signs to Route 2,3,16. Remain on 2. The road will become narrow and winding. This is the Fresh Pond Parkway. Several car dealerships and Fresh Pond Seafood will be on the right. At the 1st rotary, take the third right onto Concord Ave. Continue straight at the second rotary. Fawcett is one block further on right. Once on Fawcett St. the Newman Auditorium is about 1/2 block, on the right. Park in the lot on the right side of the street; the lot is adjacent to the auditorium building.

Public Transportation: Take the T to Harvard Square. From Harvard Square take the Concord Ave./Belmont Center bus. Get off at Fawcett St.

Real Times Acting Editors

Jim Byrd (617) 628-6859(home), byrd@acm.org
 Peter Mager (781) 890-2084, p.mager@computer.org

GBC/ACM Officers(1998 - 1999)**President**

James S. Ganino, jsganino@acm.org

Vice President

Jim Byrd (617) 628-6859(home), byrd@acm.org

Secretary

Ed Bristol, ebristol@foxboro.com

Treasurer

Stephanie Collins, jsmcollins@neu.edu

Past President

Anne Warren, (617) 495-8420, warren@hrm.harvard.edu

Local Special Interest Group Chairs**GB/SIGCHI**

Dan Workman, dan.workman@eastmansoftware.com

SIGGRAPH/Boston

Olin Lathrop, (978) 392-0881, olin@cognivis.com

GB/WEB TECH

Dennis McCarthy, (781)894-1964, maccarthy@acm.org

Standing Committee Chairs**PDS Committee**

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

Monthly Meeting Committee

Open

Publicity Committee

Joe Galligan, joegail@ibm.net

Membership Committee

Kenneth Baclawski, kenb@ccs.neu.edu

Network Services Committee

Michael Ciaraldi, ciaraldi@ciaraldi.com, <http://www.acm.org/chapters/gbc>

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 or third-class postage paid at Boston, MA 02101, Lexington, MA 02420, and other post offices.

All rights reserved: © 1999 by the Greater Boston Chapter of the ACM. Copying without fee is permitted, provided that copies are not made or distributed for direct commercial advantage and credit to the source is given, except articles that are noted otherwise. Abstracting with credit is permitted. For copying of articles that are specially noted, contact the Editor at the address below.

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.

Postmaster:

Address changes should be sent to the mailing address above. Allow eight to ten weeks for changes to address or membership renewal to become effective. Send old label with address modifications

What Happened to the April Issue?

Because of a font mismatch problem and other production delays, the April issue became so late that it was no longer worth mailing. An online version was, however, posted to the GBC web page

<http://www.acm.org/chapters/gbc>

on April 5. In general, the gbc newsletter will appear online one to two weeks before you get it in your mailbox.

We are hoping to improve the format and content of the newsletter gradually over time and are looking for people willing to contribute to both. We could particularly use someone willing to improve the copy layout and are also looking for short articles and announcements. Currently, the newsletter is, for historical reasons, being produced in PDF format using Adobe Pagemaker. In the future, we plan to also produce an HTML version, that will be posted online and periodically updated throughout the month.

One of the causes of newsletter lateness is that talk announcements are not getting to us by our usual publication date and thus causing us to hold back publication. This month, we published ontime anyway, which is reflected in the sparcity of talk announcements. To get information about talks by other groups, check out some of the web sites listed below.

Websites of some Local Groups**SIGGRAPH**

www.siggraph.org/chapters/boston

WebTech

www.acm.org/chapters/webtech

BACOM

www.netnumina.com/bacom

SPIN

www.cs.uml.edu/Boston-SPIN

IEEE Consultants Network

www.boston-consult.org

Spring 1999 PDS Program

Return this form to GBC/ACM PDS, PO Box 465, Lexington, MA 02420-0005

Seminar & Book Titles	Advance Registration	Walk-in	Enter Amount
Practical UML	\$75	\$85	
<i>UML Toolkit</i>	\$30	\$30	
Fundamentals of WWW Security	\$75	\$85	
<i>The Web Security Reference Guide</i>	\$20	\$20	
Getting Started with Swing Components	\$75	\$85	
<i>The Java Swing Book</i>	\$35	\$35	
International ACM # _____		Sub total	
GBC ID# _____ or \$10 (required)		\$10	
Pay to GBC/ACM with Check or money order Only		Total	
Batch:	Chk #	Trans. #	Date
Name:			
Employer:			
Preferred Mailing Address: Home Work			
City:		State:	Zip:
Home Phone:			
E-mail:			
Restrict use of my name to: ACM use only Prof. soc. use GBC/ACM use			

IEEE Computer Society - 6:30 pm, Thursday, May 27th, 1999
Technology Transfer in the Creation of a Commercial Hypertext Product
Julianne Chatelain, Trellix Corporation

Trellix Corporation was founded by Dan Bricklin in the fall of 1995. Other founding and early employees included designer Micah Zimring, quality & infrastructure manager Tom Baker, product manager Lisa Underkoffler, software engineers and architects Peter Levin, Buzz Kelley and George Adams, and office manager Barbara Burnham. Dan himself is probably best known to the IEEE community as the co-creator (with Bob Frankston) of the electronic spreadsheet. As the son and grandson of printers, Dan wanted to provide online text with the same turbo-charged capabilities that the spreadsheet provided to online numbers.

The team's stated goal was to create a productivity application to assist readers of business-oriented nonfiction, such as long reports. No one likes to read such reports in their entirety, and at the time, the best way to skim was to print the report. The team decided to use hypertext, plus some innovative display techniques, to facilitate an _online_ reading experience that carried over the best aspects of print reading, including the ability to easily skim while maintaining a sense of place. Events of note in the first product's development included:

- Leveraging of ideas from prior products of Dan's Software Garden
- Experimentation with not-quite-ready business technologies, to anticipate the problems of users two years hence
- A demo of "the report of the future" to venture firms
- Development of advances in online mapping, linking, and tours (directing readers' attention or re-purposing existing documents)
- Application of findings from human-computer interaction and hypertext research
- Help from a consulting neurophysiologist and a Washington Post reporter
- Experiments with Microsoft's COM architecture
- Testing the product by transforming well-known documents such as the U.S. Constitution and (later) the Independent Counsel's Report
- Creation of a free helper utility called Trelligram to address delivery issues
- Extensive usability studies, with the results fed back into the product

The speaker will draw some conclusions from the Trellix experience about key issues involved in technology transfer from the attic or academy (or both) to the marketplace. Some members of the original development team may be able to attend and share war stories or discuss these issues with the audience.

Release 1 of Trellix won a number of awards, such as "PC Week Best of Comdex - Best All-Around Application". Release 2, which shipped in 1998, is winning customers; for more information see <http://www.trellix.com> and <http://www.trelligram.com>. Dan Bricklin's web sites are <http://www.bricklin.com> (which has more software history) and <http://www.gooddocuments.com>.

Julianne Chatelain (julianne@trellix.com, <http://world.std.com/~jchat/>) has worked with interactive information since 1979, as a technical writer and a "first user" or user advocate. She first tested information usability in 1984 and software usability in 1993. Since moving to New England from California she has worked for Systems Analysis Corp., Index Technology/INTERSOLV, and Lotus Development/OneSource Information Services before joining Trellix in 1996. Her academic background is in history and science fiction writing (Clarion).

This meeting is sponsored by the Boston Chapter of the IEEE Computer Society. Meeting begins at 6:30 pm. Coffee at 6:15 pm. An optional, pay-your-own dinner follows. For more information: Marcia Nizzari, 617 856-1804 (marcia.nizzari@tfn.com).

Directions to MARCAM: Take Route 128 to the Highland Avenue, Needham, exit (the Muzi Ford exit). Turn left at the first light onto Hunting Road. Turn left at the first light onto Kendrick Street. Cross over 128, turn right at the first light onto Wells Avenue. Go about 0.2 miles to Marcam Corporation on the right side of the road at 95 Wells Avenue. Enter the building at 85 Wells Avenue, in the middle of the back of the building, as this is the closest entrance to the auditorium.

Spring 1999 PDS Program

Schedule:

8:30am - 9:00am Registration
 9:00am - 12:15pm Morning session (break at 10:30am)
 12:15pm - 1:30pm Lunch (provided on-site)
 1:30pm - 4:30pm Afternoon session (break at 2:30pm)

Registration Fees:

Seminar materials, lunch, and refreshments are included in the \$75 fee. Registrants not current members of the GBC/ACM are charged an additional \$10, and become members of the chapter for a year. This is distinct from ACM membership. Surcharge for on-site registration is \$10. Purchase orders, credit cards, faxes and e-mail cannot be accepted. Enrollment is limited and on a first come, first served basis. Early registration must be made by a check or money order at least three weeks in advance of the seminar to receive confirmation from GBC/ACM.

Location:

Edgerton Lecture Hall, MIT Building 34, Room 101 Vassar Street (about half way between Main St and Mass Ave), Cambridge, MA

Parking:

There is free parking on Vassar Street all Saturday and there is a parking structure surrounded by a parking lot at the corner of Vassar and Main.

Public Transportation:

Red line to Kendall Square. Walk west on Main Street to Vassar Street; Turn left on Vassar and walk half way to next light to building 34.

Questions:

See: <http://www.acm.org/chapters/gbc>
 or call: (781)862-1181

Saturday May 1, 1999 Getting Started with Swing Components John Zukowski

Overview:

In the beginning, there was Java's Abstract Window Toolkit (AWT): a collection of graphical user-interface (GUI) components that furnished native look-and-feel, along with some basic graphic rendering capabilities. Programmers realized that Java's AWT lacked several capabilities commonly found in modern programs. Netscape's Internet Foundation Classes (IFC) and Microsoft's Application Foundation Classes (AFC) gained popularity. Both of these provided a richer component set for use within Java programs. Their major problem was that they weren't part of the Java Core API. If you wanted to use them within an applet, each user had to download the IFC or AFC package. If you wanted to use them within an applet or application, you had to download or deliver the entire IFC or AFC package with your program. Sun added the Java Foundation Classes (JFC) to the Java core to provide a better set of GUI components and enhanced drawing capabilities usable in both JDK 1.1 and Java 2. It is the new GUI component set, called Swing, that this seminar will explore.

Who Should Attend:

This seminar is for someone that already has a basic understanding of programming Java user interfaces and wants to learn to use the Swing component set effectively.

Objectives:

This seminar will provide a detailed look at the Swing component set for existing Java programmers and describe the Model-View-Controller (MVC) and Pluggable Look-and-Feel (PLAF) architectures used by Swing. It will also give transitioning tips useful to previous AWT 1.1 developers.

Lecturer:

John Zukowski is a Software Mage with MageLang Institute. He received a B.S. in computer science and mathematics from Northeastern University and M.S. in computer science from Johns Hopkins University. He is the author of "Java AWT Reference" from O'Reilly & Associates as well as "Borland's JBuilder: No Experience Required" and "Mastering Java 1.2" from Sybex. In addition, John has authored numerous Java technologies articles and serves on the Senior Advisory Board of JavaWorld. John also is the founder of the Mid-Atlantic Java User Group, the vice-chairman of ACM's WebTech user group, and the "Focus on Java" online guide for The Mining Co.

Session Chairs: Yaz Shaghghi (yaz@draper.com) & Peter Mager (p.mager@computer.org)

Book: *The Java Swing Book* by Eckstein, Loy, and Wood, published by O'Reilly (PDS price: \$35, List \$44.95)

Books for Sale

GBC/ACM has the following books leftover from previous seminars available for sale. They are available on a first come first serve basis. Checks will be returned if the book is no longer available.

Title	Author	List Price	ACM Price	Quantity	Total
The JAVA Programming Language	Ken Arnold	\$34.38	\$25.00		
The HTML3 Manual of Style	Larry Aronson	\$24.95	\$20.00		
Inside OLE 2 (copyright 1994, w/diskettes)	Kraig Brockschmidt	\$49.95	\$10.00		
About Face: The Essentials of User Interface Design	Alan Cooper	\$29.25	\$20.00		
Working with Active Server Pages	Michael Corning	\$39.99	\$25.00		
JAVA: How to Program (with CD)	Paul Deitel	\$99.95	\$55.00		
JAVA: How to Program (book only)	Paul Deitel	\$51.00	\$40.00		
The SGML FAQ Book: Understanding the Foundation of HTML and XML	Steve DeRose	\$68.00	\$55.00		
A Discipline for Software Engineering	Watts Humphrey	\$47.29	\$35.00		
Real-Time Systems Design and Analysis	Phil LaPlante	\$69.95	\$55.00		
Concurrent Programming In Java	Doug Lea	\$39.76	\$30.00		
The C++ Programming Language, 3rd Ed	Bjarne Stroustup	\$42.99	\$30.00		
Shipping and Handling - \$4.00 per book			\$4.00		
Check Total - payable to GBC/ACM					

Name: _____

Address: _____

City/State/Zip: _____

Phone Number: _____

Check here to receive a receipt

Mail order form and check to:

Bernie Ganino, 12 Fellsmere Ave. Wakefield, MA 01880

GBC/ACM May Meeting
Thursday, May 20, 7pm
BBN/GTE, Fawcett St, Cambridge, Ma

The Mao Zedong Approach to Public Key Infrastructures

Dr. Stephen T. Kent

Chief Scientist- Information Security, BBN Technologies
 Director, Security Practice Center, GTE Internetworking
 Chief Technical Officer, CyberTrust

Continued from page 1

In his role as Chief Scientist, Dr. Kent provides oversees information security activities within BBN Technology, and works with government and commercial clients, consulting on system security architecture issues. In this capacity he has acted as system architect in the design and development of several network security systems for the Department of Defense and served as principal investigator on a number of network security R&D projects for almost 20 years. As Director of the SPC, Dr. Kent monitors all security related aspects of the service offerings of GTE Internetworking Services. He reports to the President of GTE Internetworking and coordinates with engineering, operations, and marketing to ensure the security quality of offerings. As CTO for CyberTrust Solutions, Dr. Kent provides strategic direction for this certification authority business, reporting to the General Manager of CyberTrust.

Over the last 20 years, Dr. Kent's R&D activities have included the design and development of user authentication and access control systems, network layer encryption and access control systems, secure transport layer protocols secure e-mail technology, multi-level secure (X.500) directory systems, public-key certification authority systems, and key recovery (key escrow) systems. His most recent work focuses on public-key certification infrastructures for government and commercial applications, security for Internet routing, and security for mobile computing.

The author of two book chapters and numerous technical papers on network security, Dr. Kent has served as a referee, panelist and session chair for a number of conferences. Since 1977 he has lectured on the topic of network security on behalf of government agencies, universities, and private companies throughout the United States, Europe, Australia, and the Far East.

Dr. Kent received the B.S. degree in mathematics from Loyola University of New Orleans, and the S.M., E.E., and Ph.D. degrees in computer science from the Massachusetts Institute of Technology. He is a Fellow of the ACM, a member of the Internet Society and of Sigma Xi.

IEEE Consultants Network Meeting -- WEDNESDAY, MAY 26, 7 p.m.

IS CONSULTING FOR ME? - Jeffrey M. Goldberg, Qualware Instructional Services

A down to earth interactive discussion of the ups and the downs of running a consulting practice, lead by Jeffrey Goldberg, an independent hardware, software, network consultant and educator for over ten years.

Jeffrey Goldberg is a long time innovative user of Unix and Internet services. Mr. Goldberg currently teaches courses on Unix, Shell Programming, Unix System Administration, TCP/IP Network Administration, Introduction to Programming, Visual Basic Programming, and Web Fundamentals for WPI, the IEEE, and corporate clients. He also puts together customized courses for corporate clients. Mr. Goldberg is also the principal of Quality Hardware Consulting Group, which designs electronics for fault tolerant networks, specialized network adapter hardware and embedded customized controller cards. Mr. Goldberg has recently formed a new company called Qualware Internet Services specializing in Internet Web Service, providing international advertising and home page presence twenty four hours a day for consultants, independent contractors, and companies specializing in serving other independents. This company has expertise in designing eye catching electronic advertisements for the information highway, as well as in installing and configuring a Web server for your very own.

This meeting of the Consultants' Network is scheduled for 7 p.m. Wednesday, May 26 at Arthur D. Little Co., 25 Acorn Park, Cambridge. An unsubsidized pre-meeting dinner will be held at Bertucci's at the Alewife T-Station at 5:30 PM (PROMPTLY). For more information, call the voicemail line at (781) 893-8379, e-mail to cn.boston@ieee.org, or use the Boston Chapter's BBS (781) 890-5469. If you still have questions, leave a message for Chairman Carl Frost at (508) 653-5673 or cn_chairman@qualware.com. The CN has a web page: <http://www.boston-consult.org>.