



The

UTAH TEAPOT

Winter 2002

A QUARTERLY NEWSLETTER FOR THE ALUMNI AND FRIENDS
OF THE UNIVERSITY OF UTAH SCHOOL OF COMPUTING

In This Issue

- ☒ Security of Digital Signatures
- ☒ 2002 Organick Lecture Presents David Gelernter
- ☒ Honors Program Approved
- ☒ Alumnus Profile: Eric Eide
- ☒ Robots Invade the EMCB
- ☒ U of U Intramural Cross Country Ski Race
- ☒ Tempest in the Teapot
- ☒ Salt Lake 2002
 - SOC Faculty Volunteer for Games
 - The Best Spring Break Ever
- ☒ Recent School of Computing Industry Support

The teapot was one of the first free-form models used in computer graphics. Since it was created at the University of Utah (by Martin Newell) in 1975, the teapot has become a favorite computer graphics benchmark. The teapot symbolizes Utah's distinguished leadership in computer graphics.

Security of Digital Signatures

by Lee Hollaar

You are the owner of a business, and you receive an order for widgets from another company by email. It seems in order, apparently sent by the purchasing manager of the company. But how can you know that the message is from that company's purchasing manager and the number of widgets ordered hasn't been changed, either maliciously or by accident as the email goes from machine to machine, especially if the company later denies that it sent the email?

The answer is a "digital signature" for the email, which is not a typed name or image of a conventional signature, but is a clever combination of cryptography and law that provides a way to assure that a document has not been altered or forged, and cannot later be repudiated by its creator.

To understand how a digital signature works, you need to know a little bit about public key cryptography, which is based on having two related keys with unusual properties. It is not possible to determine one key given the other, even if you know how the keys are generated and used, and either key can be used to encrypt a message and the other used to decrypt it. Normally, if you want to send a secure message to somebody using public key cryptography, you look up the public key for the person to receive the mes-

continued on page 7

2002 Organick Lecture Series Presents David Gelernter, April 17 -18, 2002

This year's lectures will be given by David Gelernter, Professor at Yale University and Chief Scientist at Mirror Worlds Technologies.

David Gelernter is Professor of Computer Science at Yale University and Chief Scientist at Mirror Worlds Technologies, New Haven, Conn. He is well known for his contributions to programming languages, distributed computing, and artificial intelligence. Dr. Gelernter is author of several books including: *Mirror Worlds*, *The Muse in the Machine*, *1939: The Lost World of the Fair*, and *Drawing a Life: Surviving the Unabomber*.

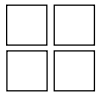
Honors Program Approved

The School of Computing gained approval for the first ever department-level honors track at the University of Utah in October 2001. Unlike the traditional liberal arts curriculum of the university-wide honors program, the Computer Science Honors Track will focus on specialized study to prepare undergraduates for graduate work in Computer Science.

In fall semester, Peter Shirley taught ten students in the first honors course ever offered in the CS program, Honors Software Practice. Fifteen students have enrolled in the honors Introduction to Computer Graphics in spring semester.



ALUMNUS PROFILE



Eric Eide started programming when he was very young, when his father taught him to write BASIC programs on the University of Utah's UNIVAC mainframe computer in the mid-1970's. Eric received his BS degree (summa cum laude) in Computer Science from the U of U in 1989 and his MS degree from the program in 1995.

Eric now works in the School of Computing as a Research Associate with the Flux Research Group, led by Prof. Jay Lepreau. Eric's research interests include programming languages, compilers, systems, and software architecture and engineering. His current research is focused on tools and techniques for integrated component-based and aspect-oriented programming of operating systems and middleware. Eric lives in the Holladay/Cottonwood area of Salt Lake City with his wife, Shellie, who also graduated from the Department of Computer Science (BS, 1992).

Utah Teapot: Why did you choose to work at the U? What's special about working in academia?

Eric Eide: I worked in industry for a while on some very interesting projects. But I returned and stayed in the School of Computing because I truly enjoy the School's environment, the people, and the benefits of working in academia. Here, I can work on exciting research projects with very smart people. Prof. Jay Lepreau, the director of the Flux Research Group, gives me the freedom to choose the projects that I work on. Jay also supports my involvement in other School activities, including the School's annual High School Computing Institute (HSCI) and High School Programming Contest. He's also given me support to work on the national and international level in program committees and NSF reviewing work.

UT: Do you work much today with

students one-on-one?

EE: The HSCI gives me the opportunity to do a little teaching, and to work with very talented high school students one-on-one. In my day-to-day position, I closely work with both graduate and undergraduate students on research projects, but as a Research Associate (research staff) I don't for-



mally supervise or teach students. I enjoy working with students at all levels: teaching, research, and being a student myself in seminars.

UT: What's been your biggest accomplishment since working here?

EE: Since becoming a Research Associate, I would say that my accomplishment with the greatest impact so far has been to distribute and publish about the "Flick" IDL compiler that we created in the Flux Research Group. Many of the ideas that we pioneered in Flick have been incorporated into commercial CORBA products, and I think we did a good job of pushing those ideas into the world. But really, I think that my greatest academic accomplishments lie ahead.

UT: What's changed the most since you were a student?

EE: The most obvious changes are centered around the Internet, of course. Being at Utah, I had access to the Internet as an undergraduate student way back when — Google tells me that my first message to USENET was sent in September 1987. The Internet used to be a luxury, but now, of course, it's so common as to be taken for granted. Access to powerful com-

puters has also changed. It used to be that universities had much more powerful workstations than students could generally buy for themselves. Now, it's often the other way around: many students have PCs that are more powerful than the lab workstations! Finally, the Internet has made it so much easier for students to find information, and this has changed education for both students and teachers.

UT: Any stories to share from the student days?

EE: Well, a bunch of students once decorated Prof. David Hanscom's car as a giant rabbit, but I'm not at liberty to name any names. And no, I don't have any pictures. Ask Dave.

UT: Tell us about your family connections to the U.

EE: My father, brother, wife, and I have all worked for different computer-related University departments over the years. We all started in the University of Utah Computer Center (UCC) but have long since been dispersed to other organizations around campus. My father works in what is now called NetCom, and my wife works for the Utah Education Network (UEN). Although both my wife and I graduated from the Department of Computer Science, we actually met in the University's marching band. I play the French horn and she plays the flute.

UT: Anything that you would you do differently?

EE: If I had known that I was going to stay in academia after graduate school, I probably would have pursued a Ph.D. instead of an MS. But this isn't a regret — my long-term involvement with the School of Computing has been a very rewarding part of my life, and I plan to be here for many years to come!

Email Eric Eide at eeide@cs.utah.edu.



Robots invade the EMCB



Mindbrew Team

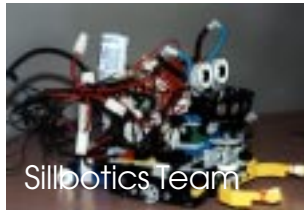
Seniors showed off their creations at a demonstration session capping off the Computer Engineering Senior Project course (CS/EE 4710), taught by Bruce Boyes, adjunct professor in Electrical Engineering and Systronix Technical Director.

Students designed robots using a JStamp™ native Java™ execution module provided by Systronix, Java software, and other components, including Lego™

Mindstorms, Lego™ Robosports kit, Lego™ rotation/angle sensor, a Devantech SRF04 Ultrasonic Range Finder, and additional sensors and motors. “Legos enable students to build sophisticated robotic and mechanical structures inexpensively and extremely rapidly,” said Boyes.

Nine teams demonstrated their projects to an audience of 75 at the end of Fall semester.

“Native-execution Java is poised to have an enormous impact on how we develop embedded systems. The JCX Lego™ interface combines unprecedented computing power with off-the-shelf robotics hardware. The Fall 2001 4710 class was the first University course in the world to use these cutting-edge tools,” said Boyes.



Sillbotics Team

SoC Prevails in Intramural Ski Races



photo by Ann Torrence

Another clean sweep for the School of Computing teams in the intramural cross-country ski races, as members won every division!

Tempest in a Teapot

By Tom Henderson
Director, School of Computing

The Core Issues of Computing

There is some evidence that computing has come a long way: everybody has and uses a computer. Our lives have become so busy, and we are connected to so many things at once, that only a computer can go fast enough to keep up. Consequently, we computer scientists spend a lot of time finding new things for computers to do: we write new programs and develop new systems and networks to support all this frantic activity. This does indeed keep us busy!

But sometimes it is useful to reflect more slowly and carefully on the deeper issues of computing: What is the nature of information and its relation to the physical or biological world? What fundamental laws govern the expression and manipulation of information? How can we characterize and handle complexity? What models of computation exist and what implementations of them are possible? Which, if any, human capabilities have an explanatory computational model? For example, can we develop computational modules to reason? To speak? To see? To love?

It is an interesting fact that work on such core issues gave rise to most computing disciplines; for example, programming languages, compilers, computer architecture, etc. However, the fundamental issues have not been completely resolved, and I urge everyone to spend some of their cycles thinking about them. Grappling with deep issues will help us better appreciate the results that have been achieved, and may even further progress. Such effort will certainly better prepare us for dealing with a broader range of problems, and will continue, no doubt, to produce new computing approaches and disciplines.

For just like an apple, the core has the seeds to future innovation - they need only be tended and developed!

Email Tom Henderson at director@cs.utah.edu

Send news items to teapot@cs.utah.edu



SoC Faculty Volunteer for 2002 Winter Games

Dave Hanscom will be the Assistant Chief of Timing for the cross-country events for both the Olympics and Paralympics. His duties will include overseeing volunteer staffing, supervising the backup timing operation, and monitoring results before they're released to the press.

"I've been organizing most of the local cross country ski races for many years.



Dave Hanscom and Al Davis

When Salt Lake City received the bid for the 2002 Winter Games, I volunteered to help select a site for the cross-country ski venue. After we'd chosen Soldier Hollow, I served on the committee that hired the architectural firm that designed the venue. In addition, I helped SLOC find a director for the cross-country skiing events, John Aalberg (one of our CS majors and a member of the UofU ski team). John asked me to help out with timing at the Olympics."

Hanscom has been preparing for his games assignment for some time, "I have been invited to participate in meetings over the past couple of years with the top dogs in the cross country skiing world. They did send me to Calgary to check out their cross country facilities a few years ago, and to Nagano in 1998, so I guess I've had a few perks."

Al Davis will be the assistant starter for the cross-country skiing events. The head starter is Pat Miller, who coached the University of Utah ski team through several national championships.

"I got involved mainly because Dave Hanscom asked me to. I've been a skier my whole life and started cross-country skiing about 25 years ago. I've always viewed the Winter Olympics as the ultimate competition," said Davis.

"The highlight will definitely be watching the best people in the world ski. We will also host the Paralympics in March, and last year we hosted a Paralympic event as well," Davis added. "In some sense, watching the dedication and skill of people with significant physical handicaps is even more inspiring than watching the regular Olympians. As far as I can tell, a guy with one leg can ski better than I could on my best day, and a blind biathlon skier can out shoot me on my best day. My advice is that if you don't feel like fighting the crowds to go to the Olympics, then you should go to the Paralympics. The price is much lower and the crowds will not be an issue. Just GO - it will give you a whole new level of appreciation for the strength of the human spirit."

John Carter will be participating in the Opening Ceremony. Since the details of the event are top-secret, he was willing only to divulge that "I'll be 'operating' one of the twenty 20-foot tall trees in the very first scene, which involves a mixture of land and ice elements. The costuming is quite intricate, and our costumes in particular were designed and imported from Latin America. We're practicing twice a week in January, including all-day practices (very tiring) on the weekends."

Look for Dave, Al and John during the games.

Best Spring Break Ever

by Brent Olson

Ah, the wonderful memories of Spring Break. One full week with nothing to do but debug a compiler that turns all numbers into 7's, fix a digital circuit that subtracts but won't add, and wire money to your psychology roommate can meet bail after "partying" a bit too much in Mexico. Weren't those the days?

This year however, School of Computing students may finally have a Spring Break so long even the cruelest professor can't fill it with homework. Thanks to the Olympics, students have February 2-26 off - the longest, coolest Spring Break ever. Literally.

With traditional hot spots still frozen solid, what will CS students do? Not surprisingly, the most common response is, "I don't know."

Though the Olympics will be bringing people from around the world to Salt Lake City, CS undergraduate Janeal Sessions plans to avoid all the Olympic hubbub and chaos like the plague. "I'm staying away from Salt Lake because I'm afraid of all the traffic," Sessions added. She does express a hope of getting down to southern Utah for a while, a sentiment many CS students seem to share.

Other CS students will be spending the break volunteering for the Olympics. Whit Johnson (CS senior) will be working at the Opening and Closing Ceremonies. "I am volunteering for the transportation team," Johnson said. The transportation team is responsible for moving people and equipment for the rehearsals and the actual ceremonies, along with ushering and greeting responsibilities.

"It's a once in a lifetime opportunity," Johnson said. "I wasn't sure if it would work out because you have to volunteer far in advance, but it works out with school being out and my work being flexible."

Steven Mosher (CE/CS junior) was called to duty through the Utah National Guard in support of the Games. He has been assigned to support the U.S. Secret Service security detail at various venues. "The Guard has made

some accommodations for me to get to school, and the faculty have been very helpful on homework assignments and projects, but its very exhausting," Mosher said.

Eric Goebel (CS senior) will work directly with the athletes themselves. "I'm helping out the Austrian Olympic team," Goebel said. "I applied to be a volunteer more than a year ago and because of my language skills they asked me to do this."

As a National Olympic Committee assistant, Goebel will be stationed in the Olympic Village and will be involved with desk-work and driving athletes to various destinations more than eight hours a day, five days a week.

"It will keep me busy," he said. "It's a chance to use my language skills and have some fun."



MILESTONES

FACULTY

Chris Johnson, Director of the SCI Institute gave talks at the Supercomputing 2001 Conference and Biocomputing 2001 Conference. He also co-chaired and hosted an NSF Workshop on Computational Science and Engineering.

STUDENTS

Five students were initiated into the Tai Beta Pi Engineering Honor Society.

- Richard C. Davidson, Computer Science
- Alan K. Morris, Computer Science
- Ryan S. Spencer, Computer Science
- John H. Thorton, Computer Science
- Jian Zhou, Computer Engineering/CS

Tai Beta Pi is the only engineering honor society is representing the entire engineering profession and the nation's second oldest honor society.

NEW FACULTY AND STAFF



Phil Willden joined the School of Computing in December 2001. In his role as Administrative Manager, Phil will be handling payroll, human resources, and accounting. Phil is a Utah native. He loves to travel and enjoys music. He has a mini-museum of Beatles memorabilia in the basement

of his house.

Marek Kowalski arrived from Cardinal Stefan Wyszyński University (formerly the University of Warsaw) to spend spring semester as Visiting Professor and holder of the Clyde Chair in the College of Engineering. He is teaching graduate seminars in Optimal Signal Recovery, and collaborating with Kris Sikorski and Frank Stenger on a monograph.



New Members of Flux Group

Edye Hoffmann returned to the School of Computing's Flux Research Group in September 2001. As Flux's Administrative Officer, aka Chief Paper Wrangler, Edye will focus on contract management and support of future research endeavors.

Robert Morelli joined the School of Computing's Flux Research Group in July 2001 as a Research Associate. His background is in mathematics, where his research

has focused on the interplay between algebraic geometry and the combinatorics of polyhedra. Robert holds a PhD in mathematics from Harvard University, and held positions at the University of Chicago and the Institute for Advanced Study in Princeton before coming to Utah.

Ian Murdock joined the School of Computing's Flux Research Group as a Research Associate in August 2001. His interests include distributed operating systems, mobile computing, and network file systems. Ian is the founder of Debian, an open source project he started in 1993 to produce one of the first Linux distributions. He is also co-founder and chairman of Progeny Linux Systems, a provider of Linux-based software and services based in Indianapolis. Ian received his BS in computer science from Purdue in 1996. He telecommutes from Fishers, Indiana, where he lives with his wife Debra and daughters Regan and Keely.

John Regehr joined the School of Computing as a postdoctoral researcher with the Flux Group in April 2001. His research interests include using real-time scheduling techniques in general-purpose operating systems, and ways to create real-time embedded systems quickly and cheaply without sacrificing performance or correctness. John received a PhD in Computer Science from the University of Virginia in May 2001.

Robert Ricci joined the School of Computing as a full-time Research Associate in August 2001, after 2.5 years of part-time employment within the College of Engineering. Robert works with the Flux Research Group on various projects including the Utah Network Testbed. Robert recently received his BS in Computer Science from the University of Utah.

Kirk Webb joined the School of Computing as a Research Associate for the Flux Group in September 2001. He works with Utah Network Testbed and other R&D. Kirk graduated from the University of Utah with a degree in Computer Engineering, and had previously worked as Senior Systems Administrator for Sarcos, Inc. His interests include composing music, backpacking, and gaming with his wife and friends on the weekends.

Brian White joined the School of Computing in September 2001 as a visiting graduate student, working with the Flux Research Group. His research interests include file systems and distributed operating systems. Brian is a graduate student at the University of Virginia and is a member of the Legion Project. He received a BS (1998) from Carnegie Mellon and an MS (2001) from the University of Virginia.

Recent School of Computing Industry Support

The School of Computing faculty and students accomplish many of their goals with generous help from our industry supporters.

3Ware, Inc.
Abstrax, Inc.
American Microsystems, Inc.
Bionic Technologies, Inc.
Borland
Cisco Systems, Inc.
Evans & Sutherland
First Security Foundation
Hazelhill Logic Solutions
Hewlett Packard Company

Intel Foundation
Lineo, Inc.
Microsoft Corporation
Novell
Nvidia
SGI
Summit Law Group
Sun Microsystems, Inc.
Systronix
Xmission

Digital Signatures

continued from page 1

sage and encrypt the message using that key. Only the person receiving the message knows the private key related to his or her public key, and therefore is the only person who can decrypt the message.

Digital signatures use public key encryption backwards. The people signing documents encrypt them with their private keys, which only they know. If a document can be decrypted using a person's public key, it must have been signed by that person. For efficiency, a checksum of the document, called a message digest, is encrypted, not the actually document. If the document is later changed, the decrypted message digest will not match that of the altered document. That's the technology behind a digital signature.

But the technology is not enough. You need an infrastructure so that you know that the public key you use to verify the digital signature of a document really belongs to the person. This is done by registering the public key with a trusted organization, called a certification authority (CA), who issues a digitally-signed document, called a certificate, that indicates that it has confirmed that a particular person has the private key corresponding to the

public key on the certificate.

That sounds exotic and complicated, but every time you access a secure web site, your browser is verifying the information sent by that site by requiring it to be signed using a digital signature, verified by a certificate from a CA on a list built into your browser.

On June 30, 2000, President Clinton signed into law the Electronic Signatures in Global and National Com-

A "digital signature" is not a typed name or image of a conventional signature, but is a clever combination of cryptography and law.

merce (E-SIGN) Act, which says that electronically-signed documents (whether by a digital signature or any other method) won't be denied legal effect just because they don't have a written signature. Thirty states (including Utah) have also passed the Uniform Electronic Transactions Act (UETA), which is intrastate counterpart to E-SIGN. These laws are limited to electronic commerce.

But the Utah Digital Signature Act goes much further. Rather than being technology-neutral like E-SIGN and UETA, it requires cryptographic digital signatures, the only technology at the time of its passage (and even now)



The Utah Teapot

A quarterly newsletter for alumni and friends of the University of Utah School of Computing.

Editor: Ann Torrence
torrence@cs.utah.edu

Asst. Editor & Layout Design:
Chris Coleman
coleman@cs.utah.edu

School of Computing
University of Utah

50 S. Central Campus Drive
Room 3190

Salt Lake City, Utah 84112-9205

Phone: 801-581-8580

Fax: 801-581-5843

<http://www.cs.utah.edu>

© 2002 University of Utah

that provides the necessary reliability. Since it is based on a particular technology, it can place important requirements on the necessary infrastructure and assure that the infrastructure will be available in the future to confirm digital signatures.

The Utah Act places digital signatures on a par with conventional signatures, recognizing them not only for electronic commerce, but also for land deeds, government proclamations, wills, court filings and orders, and anything else that must be signed. And it also treats the signed electronic document as if it were written on paper.

For more information on the Utah Act and digital signatures, see: www.commerce.state.ut.us/corporat/dsmain.htm

Lee Hollaar is a professor in the School of Computing, where he teaches data communications and networking (that includes a section on cryptography and digital signatures) and computer law. He was on the committee that drafted the Utah Digital Signature Act which, in 1995, became the first law recognizing digital signatures.

CALENDAR



January 31, 2002

Evans & Sutherland Distinguished Lecture
Leslie Pack Kaelbling, MIT Artificial
Intelligence Laboratory
Title: "Why Robbie Can't Learn: The Difficulty
in Learning Autonomous Agents"

February 2-February 26, 2002

Semester Break
XIX Olympic Winter Games

February 4, 2002

High School Computer Programming Contest

March 7-16, 2002

Salt Lake 2002 Paralympics

April 15, 2002

Application deadline for High School
Computing Institute

April 17-18, 2002

Organick Memorial Lecture Series presents
David Gelernter

- Wednesday, April 17, 2002
7:30 p.m. EMCB 104
- Thursday, April 18, 2002
3:40 p.m. EMCB 105

May 10, 2002

University Commencement and Convocation

May 20, 2002

First Summer Session begins

June 17 - July 18, 2002

High School Computing Institute



School of Computing
University of Utah
50 S Central Campus Drive
Rm. 3190 MEB
Salt Lake City, UT 84112-9205



