news@UK

The Newsletter of the UK UNIX Users Group
Published electronically at `http://www.ukuug.org/newsletter/`

Volume 11, Number 4 ISSN 0965-9412 October 2002

Contents

Report on Annual General Meeting

Jane Morrison

The Eleventh UKUUG Annual General meeting was held at the Institute of Education on 26th September: see the minutes enclosed with this mailing. The meeting was followed by a talk by Aaron Crane of GBdirect entitled “Coping with XML”.

There were four vacancies on the Council; there were four nominations. Alasdair Kergon and James Youngman were re-elected. Two new members are Sam Smith, who has handling many of our chores over this last year, and Alain Williams, who has been associated with UKUUG for many years and was EUUG Newsletter editor.

Due to other commitments Owen Le Blanc and David Hallowell resigned at this AGM and we would like to take this opportunity of thanking them for their work and interest during their time as Council members. Owen is going to stay on the Newsletter Working Group and David is going to continue his work with the UKUUG CDs.

Thanks are also due to the UKUUG book reviewers who have consistently produced book reviews of a high standard.

Membership numbers are 401 - 49 Academic, 44 Commercial, 278 Individuals, and 30 Student.

Council is also planning new Sponsorship categories, see the Chairman’s report in this newsletter for more information.

The next Newsletter will be published in December - the copy date is: 25th November. All submissions should be sent to `newsletter@ukuug.org`

UKUUG Secretariat
PO Box 37
Buntingford
Hertfordshire
SG9 9UQ
Tel: 01763 273475
Fax: 01763 273255

`office@ukuug.org`
`http://www.ukuug.org`

Council Report – Post-AGM

Charles Curran

The new Council of Management are: Charles Curran, Chairman (re-elected Sept. 2001), Roger Whittaker (elected Sept. 2000), James Youngman, Treasurer (re-elected), Alasdair Kergon (re-elected), Sam Smith, and Alain Williams. Jane says a bit more in her piece.

Council met fewer times than previously, with most business done through e-mail and telephone conference calls. The first face-to-face meeting of the new Council will be at the end of October. If you wish to contact the council, just e-mail ukuug@ukuug.org.

Since June 2001 we have been obtaining office services directly from Jane Morrison’s through her company, JMAS. The transition from the service at Owles Hall to the Manor House in Buntingford took place transparently. We owe Jane a lot for making the changeover happen so smoothly.

During this year we switched our ISP from OA5 to [University of] Manchester Computing; most of the work in this was handled by Sam Smith. We are grateful to Andrew Macpherson for the very hard work he put in to UKUUG’s Internet presence over the years.

We continue to hold some quality events although few in number: Winter Conference and Perl for Sys Admin tutorial in London; Eric Raymond with talks at City University, NetProject, and University of Oxford, as well as various press interviews; Linux 2002, Bristol, with 144 paying participants, and David Pogue on Mac OS X at the beginning of September.

The Newsletter has now changed its production process completely. Now we need extra help with including good content.

The Working Groups are still not really off the ground; we need members to participate in these and make things happen. Please!

The register of members currently shows 401 paid members [422 members last year [432 previous year]] and 6 honorary members. These are classed as corporate 93 [94 [107]] (academic 49 [46 [55]], commercial 44 [48 [52]]), individual 278 [247 [221]] and student 30 [24 [16]].

UKUUG Open Source Award 2003

Charles Curran

Once again we are offering a prize for a significant contribution to the free and open source community; this might be in the form of an article or paper, software product, or other contribution. Its value is £ 500. Additionally, O'Reilly will pay for the winner to attend its 2003 Open Source Convention in the US.

The closing date for submissions is Friday, 2 May 2003. The prize is open to current students in UK Higher Education.

Membership Classes – Sponsors

Charles Curran

Since earlier this year, there have been discussions among UKUUG's Council about the possibilities and benefits of there being a Sponsoring class of membership.

As mentioned at the AGM, 2002-09-26, we now hope to introduce this during the coming year. Council debated having a wide range of categories but, initially, we have decided to keep things simple and just use two categories: Gold and Silver.

This is what we propose:

SILVER MEMBERSHIP: Price: £ 1,000 p.a.

Benefits:

Web link on UKUUG Sponsors' web page;

Conferences: 'free' space or table-top at each conference including two personnel;

Insert/flyer with one newsletter p.a.;

Prestige of being a Sponsor Member of UKUUG.

GOLD MEMBERSHIP: Price: £ 5,000+ p.a.

Benefits:

In addition to all of Silver Membership benefits,

Conferences: full access (up to 6 personnel) at any event, space/table-top,

own brochure in delegate bags,

mention in conference publicity of involvement;

Insert/flyer with each newsletter;

Prestige of being a Gold a Sponsor Member of UKUUG.

We will remind such sponsors of our vendor-independent stance and ask that their involvement in UKUUG events and items they ask UKUUG to publish are in accordance with UKUUG's principles and at least of general relevance to our membership.

If you have strong views on this, please send them to the Secretariat.

UKUUG Linux Developers' Conference 2003 - Call for Papers

EDINBURGH 2003

Planning for the 2003 Linux Developers' Conference is already underway and again we are seeking ideas, speakers and sponsors.

We would like to invite speakers on all types of Linux development to contribute. The programme will cover a variety of subjects, including kernel and desktop development, tools, applications, and networking. Any topic likely to be of interest to Linux developers and enthusiasts will be considered.

The topics presented in recent years have included: ARM Linux, Clustering, CORBA, Debian Package Management, Enterprise Filesystems, Exim, GNOME, I20, Mail Servers, Memory Management, Performance Programming, Samba, Security, SMP, and VMware.

Further details of earlier conferences can be seen at
`http://www.linux.ukuug.org/linux99/`
`http://www.ukuug.org/events/linux2000/`
`http://www.ukuug.org/events/linux2001/`

and of course at
`http://www.ukuug.org/events/linux2002`

Initial abstracts should be submitted to the conference organisers electronically using the form on the Linux 2003 website at
`http://www.ukuug.org/events/linux2003/CFP/`

Abstracts should be accompanied by a short biography, and, ideally, should be about 250-500 words long. Final papers should normally last about 40 minutes, including 10 minutes for questions and answers. If you need more time for your presentation, please tell us when you submit your abstract. We shall acknowledge all submissions.

Significant dates:

Closing date for abstracts: 16th March 2003
Accepted authors notified by: 7th April 2003
Final papers due by: 18th May 2003

Particular queries should be sent either to the UKUUG office, or to the Linux 2003 mailing list
`linux2003@ukuug.org`

To keep the conference fees low, we are seeking sponsors and exhibitors. For further information about sponsoring, exhibiting, or attending the event please contact the UKUUG office:
`office@ukuug.org`

Telephone: 01763 273475

Information about the event will be updated on a regular basis on the website:
`http://www.ukuug.org/events/linux2003/`

Desktop *nix Users Find No Solution in OS X

J Paul Reed

Tim O'Reilly, founder of the popular books with animals on the cover, recently wrote an article on people switching to Mac OS X. He provides some anecdotal evidence – which, to his credit, he cites as such – about the makeup of users adopting the new OS, and attempts to make the case that Mac OS X is Unix on the desktop, achieving what Linux and numerous other Unix vendors have failed to do. But O'Reilly's claim that Apple has achieved a desktop flavour of Unix in OS X (and should focus some marketing effort on converting Unix/Linux users) dances around a number of issues, not the smallest of which is one extremely important fact: Mac OS X is not Unix.

Let me repeat that: OS X is not Unix.

Consider the following: all of Apple.com's marketing pages on the subject of their darling new operating system are extremely careful to note that OS X is "UNIX-based". While the foundation of the operating system is Darwin, a BSD-based kernel, the core of the operating system is NeXT; just ask all the hardcore Unix users who have tried to change their OS X settings using configuration files in `/etc` , only to find all their changes ignored. Apple's Unix-like operating system uses NetInfo, for a configuration datastore, something more akin to the Windows registry we all know and hate.

Consider, too, that any Unix users poking around an OS X box will be surprised to find a ”Unix” with no gcc. Or gdb. Original versions didn't even have bash. And Unix's beloved fortune, who dutifully greets us upon login, is missing. That's because all of those utilities that arguably make a "Unix system" a Unix system don't come by default with OS X; users who care about these tools will need to find the Developer's Tools CD, which Apple is nice enough to ship with OS X, but which is not part of the operating system distribution. At least "Terminal.app", featuring "vt100/vt220 emulation on par with xterm", is there.

Speaking of xterm, where is X? You know, that often-maligned client/server hardware-independent platform MIT came up with to provide GUI services for *nix while Steve was still getting his Xerox knockoff right so Bill had something to steal? You won't find it in OS X by default. "Display PDF" provides the pretty pictures for OS X users to drool over, but if you need to run that X application, you have to find yourself an X server for Mac OS X, which Apple doesn't even want to acknowledge exists (but thanks to the XDarwin project, OS X users have something to run Unix programs on their "Unix" boxes).

I could go on with stories about Unix users who expected OS X to live up to the marketing hype (my favourite being that you have to "enable" the root user before you can login as root... "Unix" indeed) and were unpleasantly surprised.

To be clear: It's not that being a Unix-based operating system is bad. In fact, most OS X users will point out that my operating system of choice, Linux, isn't really Unix either, and they're right. But while the kernel is merely Unix-like, show me a Linux distribution that doesn't ship gcc, gdb, X, and all those other utilities (even fortune) that make Unix Unix.

Further, show me a Linux distribution that ignores `/etc` and stores its configuration data in a binary registry. Linux may not be Unix, but it is so rooted in a Unix heritage that it is in a position to offer its users a "Unix" desktop environment. Contrast this to OS X, which, for all of its praises, can never provide a "desktop environment for Unix". You can't give your users something you don't have.

Another weakness inherent in O'Reilly's argument that OS X is the future of desktop Unix reveals itself in his painstaking coverage of those who switched to OS X. If we were to believe his analysis, the KDE devs might as well all go get "real" jobs, since users are moving "in droves" to OS X for their desktop experience. A closer look at their stories betrays their motives, which reveal that they weren't using Linux for the right reasons and never really "grokked" the platform.

Putting aside those who upgraded to OS X and those who migrated from Windows (we all know why they switched), the complaints of those who moved to OS X from Unix/Linux seem to fall into two categories: "User experience" on the Linux desktop isn't "there" and application support isn't always available for Unix/Linux.

Let's look at applications first. We all buy computers to get work done, and applications are the vehicle for accomplishing this. The two most popular applications you hear Mac OS X users raving about "just working" on their Macintosh come from the same company that Apple tried to go head to head with... and, like so many others, failed miserably. Unlike those now non-existent companies, Apple realized it before Microsoft cut off their air supply and went crying back to the monopolist like a dog with its tail between its legs to get Office.X and Internet Explorer ported so OS X didn't go the way of OS/2.

There is a special irony in the fact that these OS X users would support and, in some cases, highly praise a vendor they supposedly dislike so much for everything from technical to philosophical reasons. It suggests that OS X users switching from Unix on the desktop should never have switched to Unix on their desktops in the first place; you don't exactly switch to Linux for application support. Would they blame Wolfgang Puck for his sub-par cooking skills if they went to his restaurant looking for a gourmet Chinese dinner? The same invalid blame is placed when they fault Linux for their disappointment in what they perceive as a sub-par desktop experience when they were expecting clones of their Windows or OS 9 experiences.

The second category lies in the nebulous "user experience" realm. O'Reilly's testimonials include phrases like "[OS X] just works" or "Computing is fun again" or "[OS X] doesn't suck". Looking past loaded words, they don't mean anything. My Linux box, with its AfterStep desktop "just works". I've only recently begun to appreciate how fun and cool my Linux workstation is when I'm running gaim and Mozilla off my desktop at home, bounced through Solaris and HP-UX servers to a lab on campus. iTunes isn't "fun". That's fun, and it "just works".

A few of O'Reilly's testimonies do give some concrete examples of user problems they had: "I refuse to spend weekends and late nights fiddling, Linux-hacker-style, with the scripts and codes and config files...". This sentiment reinforces that these users shouldn't have been using Linux in the first place. Like most long time-Linux users, I know the pain of spending what seems like endless "cycles" trying to figure something out. But unlike other operating systems, once I hack those "scripts and codes and config files", it all "just works", and it continues to "just work" until I introduce a new variable into the equation. This is different from other desktop operating systems, OS X included, under which an application modifying something somewhere in some binary NetInfo registry could break something else. In other words, all that fiddling time may be annoying, but it is not for naught. Linux is very much a "configure once, run forever" operating system.

One of the "switchers" O'Reilly profiles likens the Linux desktop to a "typical British sports car from the 70s: Lots of engine, but it has a lousy paint job. The car 'mostly' runs, but the electrical system is erratic", while OS X is a "Mazda Miata: Stylish [and] sexy...". But Linux was never meant to be a sports car; I like to think of my Linux desktop more as an expandable VW bus towing a boat behind it and an SUV behind that. You don't really have the urge to "lick" it, but it does make you say "Damn... that's pretty cool", and you still have room for twenty more people and another car behind the SUV. See how far you get in your Miata when you try to stuff five people in it and attach a boat.

The final clue that O'Reilly's users shouldn't have been using Linux for their desktops is not what they said, but what they didn't say. Not one ex-Linux OS X user mentioned anything about freedom. I'm not referring to some Stallmanesque argument about whether the "GNU" goes before, after, or behind the "Linux", but rather my ability to look at the source code and find out exactly what it's doing if I need to, from the kernel on up. (Before OS X users mention the "Open Source" Darwin kernel, show me the source to Display PDF.) I can verify that applications aren't sending information off to Apple (or Microsoft). I can work and play on my Linux desktop without ever fearing that Linus will send me a cease and desist order for making my desktop look a certain way or telling the truth. And because my platform isn't controlled by a public corporation, I know that Linus won't slip some nefarious clause into a EULA because a majority of stockholders thinks it will maximize their profits. OS X users make a huge deal out of their beautiful, lickable desktop "just working", but the cost of this "convenience" is their freedom, both in terms of liberty and technical flexibility. For many Linux users, that's too high a price.

A "desktop environment" is many different things to different users of different platforms. It is unfair and invalid for current OS X users to fault the Linux desktop for shortcomings they perceived as they mistook a 747 for a (admittedly stylish, but smaller) Leer jet. The development of a "desktop environment" on Linux, in the form of KDE, Gnome, and – in the tradition of Open Source – software we haven't heard of yet, will continue and is of value to those who are using the Linux platform for the right reasons in the first place.

O'Reilly is wrong about Apple's possible markets. Apple may have a market in desktop users who want some of the stability and flexibility a Unix-based operating system affords them. They may even have a market in Unix users who want a desktop-focused platform for their home or desk at work, but they will never find one in Unix/Linux users who want a desktop environment.

Thanks Tim, but we already have a number of pretty damn good ones.

Reprinted by permission of the author. J Paul Reed is a Computer Science Senior at California Polytechnic State University, San Luis Obispo. When he's not hacking on the email notification component of Bugzilla or managing OpenRatings, he's been known to volunteer for the campus LUG, TA for the department's Unix Systems Programming course, and, sometimes, even attend class. He's looking to continue the research he's started in computer systems security and software engineering in graduate school next year.

What's been happening in the BSD World?

Sam Smith

The BSDs: Sophisticated, Powerful and (Mostly) Free (Lather, Rinse, Repeat)
`http://www.ukuug.org/masl/7`

Any code is only as good as its programmers
`http://www.wired.com/wired/archive/10.09/view.html?pg=3`

Michael Lucas wrote a very informative article on using groups
`http://www.ukuug.org/masl/9`

Michael Lucas's book on BSD, and FreeBSD in particular
`http://www.AbsoluteBSD.com/`

Mac OS X 10.2 - Jaguar, released to general acclaim (Ooh, shiny)
`http://www.apple.com/macosx/`
`http://www.ukuug.org/events/pogue/`

BSDCon Europe Schedule and Pricing announced. (Should be fun) Details and Early Registration:
`http://2002.eurobsdcon.org/`

Talks and Speakers:
`http://2002.eurobsdcon.org/timeschedule.html`

Interesting study on the people behind Open Source software.
`http://www.infonomics.nl/FLOSS/report/`

DarwinPorts initially released (Ports/PkgSrc alike for Darwin).

http://www.opendarwin.org/projects/darwinports/
http://www.opendarwin.org/

OpenSSL becoming Non-Free? (Some say yes. Some say no.) Theo de Raadt's inital comments...
http://www.ukuug.org/masl/1

... and the resulting discussion
http://www.ukuug.org/masl/2

NetBSD's take:
http://www.ukuug.org/masl/3

Crytography@wasabisystems' take:
http://www.ukuug.org/masl/4

NetBSD 1.6 is out(39 architectures for one release is a lot)
http://www.netbsd.org/

NetBSD 1.4 – End of Life ("NetBSD 1.6 marks the end-of-life for NetBSD 1.4")
http://www.netbsd.org/

NetBSD-current now fully dynamically linked (and the sky is not falling down)
http://www.ukuug.org/masl/5

IRIX Binary Compatability on NetBSD.
http://www.ukuug.org/masl/10

NetBSD/macppc now supports multiple processors
http://www.ukuug.org/masl/6

FreeBSD and Multimedia
http://www.ukuug.org/masl/8
http://www.onlamp.com/lpt/a/2707

Sudo Aliases and Exclusions
http://www.onlamp.com/lpt/a/2704

Developers' Want Lists (The FreeBSD list is new. The OpenBSD list has new entries)
http://www.FreeBSD.org/donations/wantlist.html
http://www.openbsd.org/want.html

Embracing the Daemon - Parts 1 and 2 ("A Special Breed of Idiot?")
http://www.ukuug.org/masl/11

Trojan'ed Unofficial OpenBSD CDs being sold (and the moral is, buy the official sets)
http://www.ukuug.org/masl/12

Checklist of security settings on FreeBSD servers
http://sddi.net/FBSDSecCheckList.html

netproject - Autumn 2002 Newsletter

Eddie Bleasdale

The issue of "Trusted Computing" has hit the headlines with the TCPA (Trusted Computing Platform Alliance) announcing the design of computers that use the TCPA chip. The purpose of TCPA is to ensure the integrity of the software on the computer. The issue has generated a heated debate - is it a way the software vendors can ensure total control over what can and can not run on your computers? or does it provide the hardware required to enable secure e-business?

Ross Anderson's views are at:
http://www.cl.cam.ac.uk/users/rja14/tcpa-faq.html

for a counter argument visit:
http://www.theregister.co.uk/content/6/26612.html

for what Microsoft is doing visit:

`http://www.microsoft.com/presspass/features/2002/jul02/07-01palladium.asp`

What is sure is that this issue is one that all involved with IT strategy can not afford to ignore. Not only will TCPA computers have the TCPA chip (known as the Fritz chip) but also a secure operating system must have a publically defined and secure application program interface, the removal of all hidden APIs. Macros, which are a security weakness have no role in a trusted system. File structures must support read, write and execute privileges.

The issue of trusted computing is one that netproject has been working on for several years and the issues are ones that we will be addressing in workshops, tutorials and conferences over the next year.

We have now established our development centre, in Cambridge, headed up by Steve Hnizdur with Sean Atkinson doing software development. Steve was the IT director for a UK insurance company and while there deployed Linux and Unix throughout the organisation - including deploying Linux on the desktop.

Sean, when at Cambridge University, contributed to the development of the Gnumeric spread sheet and has a very close relationship with the GNOME developers. Sean worked for AT&T Research on VNC and the development of 'follow me' computing - where users can wander from computer to computer and have their session following them. This is a requirement for the work we are doing for several clients and we are aiming to achieve this over the next year.

netproject has been working with the UK Police IT Organisation on the issues of deploying Linux workstations for secure computing. Police forces have a requirement for a secure, stateless, desktop computer which can be used by any authorised user. To meet these needs we have developed a Linux desktop computer that uses smart cards for log on. All the users files are held on a central server. Authentication to be achieved using a central server. These computers are being manufactured to our design by a Taiwanese company GCI who also supply and support the hardware. First systems have are now being evaluated by several organisations.

Put into your diary the dates for the next public workshops that we will be running. These include:

10th October - Planning your Directory

By Dr Andrew Findlay on how to plan for the use of LDAP servers in your organisation. What they offer, what they don't and how to go about the implementation and administration of you directory services.

23rd October - Trusted Computing Platform Alliance

What the TCPA is about. Is it a threat or is it the way to achieve secure computing. Speakers to include Alan Cox, Ross Anderson, Bill Thompson. Microsoft have also been invited to give a presentation on the Palladium initiative.

21st November - Open Source - co-existing with Microsoft

When moving to Linux and Open Source it is essential to enable inter-working with existing proprietary systems. This workshop will deal with the issues of integrating Linux and Open Source into existing, proprietary, systems and the tools that enable the smooth migration to Linux - including on the desktop.

10th December - Building a network of directory servers

Dr Andrew Findlay will moderate this practical workshop. Delegates should bring their own Laptop computers, running both their operating system of choice and directory server software. Over the day with a combination of tutorials and practical sessions the delegates will get their LDAP servers inter-working with the other delegates on the course.

23rd Jan 2003 - Linux for business

This event is our annual Open Source conference which always proves to be very popular. Two streams - one addressing the business issues the other the technology. Small exhibition of the major vendors. Day rounded of with a reception with jazz band.

Eddie Bleasdale netproject 124 Middleton Road, Morden, Surrey, SM4 6RW Tel: +44 (0)20 8715 0072

TCPA / Palladium Frequently Asked Questions (version 1.0)

Ross Anderson

1. What are TCPA and Palladium?

TCPA stands for the Trusted Computing Platform Alliance, an initiative led by Intel. Their stated goal is ‘a new computing platform for the next century that will provide for improved trust in the PC platform.’ Palladium is software that Microsoft says it plans to incorporate in future versions of Windows; it will build on the TCPA hardware, and will add some extra features.

2. What does TCPA / Palladium do, in ordinary English?

It provides a computing platform on which you can’t tamper with the applications, and where these applications can communicate securely with the vendor. The obvious application is digital rights management (DRM): Disney will be able to sell you DVDs that will decrypt and run on a Palladium platform, but which you won’t be able to copy. The music industry will be able to sell you music downloads that you won’t be able to swap. They will be able to sell you CDs that you’ll only be able to play three times, or only on your birthday. All sorts of new marketing possibilities will open up.

TCPA / Palladium will also make it much harder for you to run unlicensed software. Pirate software can be detected and deleted remotely. It will also make it easier for people to rent software rather than buying it; and if you stop paying the rent, then not only does the software stop working but so may the files it created. For years, Bill Gates has dreamed of finding a way to make the Chinese pay for software: Palladium could be the answer to his prayer.

There are many other possibilities. Governments will be able to arrange things so that all Word documents created on civil servants’ PCs are ‘born classified’ and can’t be leaked electronically to journalists. Auction sites might insist that you use trusted proxy software for bidding, so that you can’t bid tactically at the auction. Cheating at computer games could be made more difficult.

There is a downside too. There will be remote censorship: the mechanisms designed to delete pirated music under remote control may be used to delete documents that a court (or a software company) has decided are offensive - this could be anything from pornography to writings that criticise political leaders. Software companies can also make it harder for you to switch to their competitors’ products; for example, Word could encrypt all your documents using keys that only Microsoft products have access to; this would mean that you could only read them using Microsoft products, not with any competing word processor.

3. So I won’t be able to play MP3s on my PC any more?

With existing MP3s, you may be all right for some time. Microsoft says that Palladium won’t make anything suddenly stop working. But a recent software update for Windows Media Player has caused controversy by insisting that users agree to future anti-piracy measures, which may include measures that delete pirated content found on your computer. Also, some programs that give people more control over their PCs, such as VMware and Total Recorder, are unlikely to work under TCPA. So you may have to use a different player - and if your player will play pirate MP3s, then it seems unlikely to be authorised to play the new, protected, titles.

It is up to an application to set the security policy for its files, using an online policy server. So Media Player will determine what sort of conditions get attached to protected titles, and I expect Microsoft will do all sorts of deals with the content providers, who will experiment with all sorts of business models. You might get CDs that are a third of the price but which you can only play three times; if you pay the other two-thirds, you'd get full rights. You might be allowed to lend your copy of some digital music to a friend, but then your own backup copy won't be playable until your friend gives you the main copy back. More likely, you will not be able to lend music at all. These policies will make life inconvenient for some people; for example, regional coding might stop you watching the Polish version of a movie if your PC was bought outside Europe.

This could all be done today - Microsoft would just have to download a patch into your player - but once TCPA / Palladium makes it hard for people to tamper with the player software, and easier for Microsoft to control upgrades and patches, it will be harder for you to escape, and will therefore be a more attractive way of doing business.

4. How does it work?

TCPA provides for a monitoring and reporting component to be mounted in future PCs. The preferred implementation in the first phase of TCPA is a 'Fritz' chip - a smartcard chip or dongle soldered to the motherboard.

When you boot up your PC, Fritz takes charge. He checks that the boot ROM is as expected, executes it, measures the state of the machine; then checks the first part of the operating system, loads and executes it, checks the state of the machine; and so on. The trust boundary, of hardware and software considered to be known and verified, is steadily expanded. A table is maintained of the hardware (audio card, video card etc) and the software (O/S, drivers, etc); Fritz checks that the hardware components are on the TCPA approved list, that the software components have been signed, and that none of them has a serial number that has been revoked. If there are significant changes to the PC's configuration, the machine must go online to be re-certified. The result is a PC booted into a known state with an approved combination of hardware and software (whose licences have not expired). Control is then handed over to enforcement software in the operating system - this will be Palladium if your operating system is Windows.

Once the machine is in this state, Fritz can certify it to third parties: for example, he will do an authentication protocol with Disney to prove that his machine is a suitable recipient of 'Snow White'. This will mean certifying that the PC is currently running an authorised application program - MediaPlayer, DisneyPlayer, whatever. The Disney server then sends encrypted data, with a key that Fritz will use to unseal it. Fritz makes the key available only to the authorised application and only so long as the environment remains 'trustworthy'. For this purpose, 'trustworthy' is defined by the security policy downloaded from a server under the control of the application owner. This means that Disney can decide to release its premium content to a given media player application in return for a contract that the application will not make any unauthorised copies of content, will impose a certain set of conditions (including what level of security has to be set in TCPA). This can involve payment: Disney might insist, for example, that the application collect a dollar every time you view the movie. In fact, the application itself can be rented too, and this is of great interest to software companies. The possibilities seem to be limited only by the marketers' imagination.

5. What else can TCPA and Palladium be used for?

TCPA can also be used to implement much stronger access controls on confidential documents. For example, an army might arrange that its soldiers can only create Word documents marked at 'Confidential' or above, and that only a TCPA PC with a certificate issued by its own security agency can read such a document. This is called 'mandatory access control', and governments are keen on it. The Palladium announcement implies that the Microsoft product will support this: you will be able to configure Word so that it will encrypt all documents generated in a given compartment on your machine, and share it only with other users in a defined group.

Corporations will be able to do this too, to make life harder for whistleblowers. They can arrange that company documents can only be read on company PCs, unless a suitably authorised person clears them for export. They can also implement timelocks: they can arrange, for example, that all emails evaporate after 90 days unless someone makes a positive effort to preserve them. (Think of how useful that would have been for Enron, or Arthur Andersen, or for Microsoft itself during the antitrust case.) The Mafia might use the same facilities: they could arrange that the spreadhseet with the latest drug shipments can only be read on accredited Mafia PCs, and will vanish at the end of the month. This might make life harder for the FBI - though Microsoft is in discussions with governments about whether policemen and spies will get some kind of access to master keys. But, in any case, a whistleblower who emails a document to a journalist will achieve little, as the journalist's Fritz chip won't give him the key to decipher it.

TCPA / Palladium also seems destined for use in electronic payment systems. One of the Microsoft visions appears to be that much of the functionality now built on top of bank cards may move into software once the applications can be made tamper-resistant. This is needed if we are to have a future in which we pay for books that we read, and music we listen to, at the rate of so many pennies per page or per minute. Even if this doesn't work out as a business model - and there are good arguments why it won't - there is clearly a competitive issue for a number of online payment systems, and there may be spillover effects for the user. If, in ten years' time, it's inconvenient to shop online with a credit card unless you use a TCPA or Palladium platform, then this could move a lot of people over to the system.

6. OK, so there will be winners and losers - Disney might win big, and smartcard makers might go bust. But surely Microsoft and Intel are not investing nine figures just for charity? How do they propose to make money out of it?

My spies at Intel tell me that it was a defensive play. As they make most of their money from PC microprocessors, and have most of the market, they can only grow their company by increasing the size of the market. They are determined that the PC will be the hub of the future home network. If entertainment is the killer application, and DRM is going to be the critical enabling technology, then the PC has to do DRM or risk being displaced in the home market.

Microsoft were also motivated by the desire to bring all of entertainment within their empire. But they also stand to win big if either TCPA or Palladium becomes widespread, as they will be able to use it to cut down dramatically on software copying. 'Making the Chinese pay for software' has been a big thing for Bill; with Palladium, he can tie each PC to its individual licenced copy of Office, and with TCPA he can tie each motherboard to its individual licenced copy of Windows. TCPA will also have a worldwide blacklist for the serial numbers of any copies of Office that get pirated.

Finally, Microsoft would like to make it more expensive for people to switch away from their products (such as Office) to rival products (such as OpenOffice). This will enable them to charge more for upgrades without making their users jump ship.

7. Where did the idea come from?

It first appeared in a paper by Bill Arbaugh, Dave Farber and Jonathan Smith, "A Secure and Reliable Bootstrap Architecture", in the proceedings of the IEEE Symposium on Security and Privacy (1997) pp 65-71. It led to a US patent: "Secure and Reliable Bootstrap Architecture", U.S. Patent No. 6,185,678, February 6th, 2001. Bill's thinking developed from work he did while working for the NSA on code signing in 1994. The Microsoft folk have also applied for patent protection on the operating system aspects. (The patent texts are here andhere.)

There may be quite a lot of prior art. Markus Kuhn wrote about the TrustNo1 Processor years ago, and the basic idea - a specially trusted 'reference monitor' that supervises a computer's access control functions - goes back at least to a paper written by James Anderson for the USAF in 1972. It has been a feature of US military secure systems thinking since then.

8. How is this related to the Pentium 3 serial number?

Intel started an earlier program in the mid-1990s that would have put the functionality of the Fritz chip inside the main PC processor, or the cache controller chip, by 2000. The Pentium serial number was a first step on the way. The adverse public reaction seems to have caused them to pause, set up a consortium with Microsoft and others, and seek safety in numbers.

9. Why call the monitor chip a 'Fritz' chip?

In honour of Senator Fritz Hollings of South Carolina, who is working tirelessly in Congress to make TCPA a mandatory part of all consumer electronics.

10. OK, so TCPA stops kids ripping off music and will help companies keep data confidential. It may help the Mafia too, unless the FBI get a back door, which I assume they will. But apart from pirates, industrial spies and activists, who has a problem with it?

A lot of companies stand to lose out. For example, the European smartcard industry looks likely to be hurt, as the functions now provided by their products migrate into the Fritz chips in peoples' laptops, PDAs and third generation mobile phones. In fact, much of the information security industry may be upset if TCPA takes off. Microsoft claims that Palladium will stop spam, viruses and just about every other bad thing in cyberspace - if so, then the antivirus companies, the spammers, the spam-filter vendors, the firewall firms and the intrusion detection folk could all have their lunch stolen.

There are serious concerns about the effects on the information goods and services industries, and in particular on innovation, on the rate at which new businesses are formed and on the likelihood that incumbent companies will be able to hang on to their monopolies. The problems for innovation are well explained in a recent New York Times column by the distinguished economist Hal Varian.

But there are much deeper problems. The fundamental issue is that whoever controls the Fritz chips will acquire a huge amount of power. Having this single point of control is like making everyone use the same bank, or the same accountant, or the same lawyer. There are many ways in which this power could be abused.

11. How can TCPA be abused?

One of the worries is censorship. TCPA was designed from the start to support the centralised revocation of pirate bits. Pirate software will be spotted and disabled by Fritz when you try to load it, but what about pirated songs or videos? And how could you transfer a song or video that you own from one PC to another, unless you can revoke it on the first machine? The proposed solution is that an application enabled for TCPA, such as a media player or word processor, will have its security policy administered remotely by a server, which will maintain a hot list of bad files. This will be downloaded from time to time and used to screen all files that the application opens. Files can be revoked by content, by the serial number of the application that created them, and by a number of other criteria. The proposed use for this is that if everyone in China uses the same copy of Office, you do not just stop this copy running on any machine that is TCPA-compliant; that would just motivate the Chinese to use normal PCs instead of TCPA PCs in order to escape revocation. So you also cause every TCPA-compliant PC in the world to refuse to read files that have been created using this pirate program.

This is bad enough, but the potential for abuse extends far beyond commercial bullying and economic warfare into political censorship. I expect that it will proceed a step at a time. First, some well-intentioned police force will get an order against a pornographic picture of a child, or a manual on how to sabotage railroad signals. All TCPA-compliant PCs will delete, or perhaps report, these bad documents. Then a litigant in a libel or copyright case will get a civil court order against an offending document; perhaps the Scientologists will seek to blacklist the famous Fishman Affidavit. Once lawyers and government censors realise the potential, the trickle will become a flood.

Now the modern age only started when Gutenberg invented movable type printing in Europe, which enabled information to be preserved and disseminated even if princes and bishops wanted to ban it. For example, when Wycliffe translated the Bible into English in 1380-1, the Lollard movement he started was suppressed easily; but when Tyndale translated the New Testament in 1524-5, he was able to print over 50,000 copies before they caught him and burned him at the stake. The old order in Europe collapsed, and the modern age began. Societies that tried to control information became uncompetitive, and with the collapse of the Soviet Union it seemed that democratic liberal capitalism had won. But now, TCPA and Palladium have placed at risk the priceless inheritance that Gutenberg left us. Electronic books, once published, will be vulnerable; the courts can order them to be unpublished and the TCPA infrastructure will do the dirty work.

So after the Soviet Union's attempts to register and control all typewriters and fax machines, TCPA attempts to register and control all computers. The implications for liberty, democracy and justice are worrying.

12. Scary stuff. But can't you just turn it off?

Sure - unless your system administrator configures your machine in such a way that TCPA is mandatory, you can always turn it off. You can then run your PC with administrator privileges, and use insecure applications.

There is one respect, though, in which you can't turn Fritz off. You can't make him ignore pirated software. Even if he's been informed that the PC is booting in untrusted mode, he still checks that the operating system isn't on the serial number revocation list. This has implications for national sovereignty. If Saddam is stupid enough to upgrade his PCs to use TCPA, then the American government will be able to hot-list his Windows licences, and thus shut down his PCs, next time there's a war. Booting in untrusted mode won't help. He'd have to dig out old copies of Windows 2000, change to GNU/linux, or find a way to isolate the Fritz chips from his motherboards without breaking them.

If you aren't someone the US President hates personally, this may not be an issue. But if you turn TCPA off, then your TCPA-enabled applications won't work, or won't work as well. It will be like switching from Windows to Linux nowadays; you may have more freedom, but end up having less choice. If the applications that use TCPA / Palladium are more attractive to the majority of people, you may end up simply having to use them - just as many people have to use Microsoft Word because all their friends and colleagues send them documents in Microsoft Word. Microsoft says that Palladium, unlike vanilla TCPA, will be able to run trusted and untrusted applications at the same time in different windows; this will presumably make it easier for people to start using it.

13. So economics are going to be significant here?

Exactly. The biggest profits in IT goods and services markets tend to go to companies that can establish platforms (such as Windows, or Word) and control compatibility with them, so as to manage the markets in complementary products. For example, some mobile phone vendors use challenge-response authentication to check that the phone battery is a genuine part rather than a clone - in which case, the phone will refuse to recharge it, and may even drain it as quickly as possible. Some printers authenticate their toner cartridges electronically; if you use a cheap substitute, the printer silently downgrades from 1200 dpi to 300 dpi. The Sony Playstation 2 uses similar authentication to ensure that memory cartridges were made by Sony rather than by a low-price competitor.

TCPA appears designed to maximise the effect, and thus the economic power, of such behaviour. Given Microsoft's record of competitive strategic plays, I expect that Palladium will support them. So if you control a TCPA-enabled application, then your policy server can enforce your choice of rules about which other applications will be allowed to use the files your code creates.

These files can be protected using strong cryptography, with keys controlled by the Fritz chips on everybody's machines. What this means is that a successful TCPA-enabled application will be worth much more money to the software company that controls it, as they can rent out access to their interfaces for whatever the market will bear. So there will be huge pressures on software developers to enable their applications for TCPA; and if Palladium is the first operating system to support TCPA, this will give it a competitive advantage over GNU/Linux and MacOS with the developer community.

14. But hang on, doesn't the law give people a right to reverse engineer interfaces for compatibility?

Yes, and this is very important to the functioning of IT goods and services markets; see Samuelson and Scotchmer, "The Law and Economics of Reverse Engineering", Yale Law Journal, May 2002, 1575-1663. But the law in most cases just gives you the right to try, not to succeed. Back when compatibility meant messing around with file formats, there was a real contest - when Word and Word Perfect were fighting for dominance, each tried to read the other's files and make it hard for the other to read its own. However, with TCPA that game is over; without access to the keys, or some means of breaking into the chips, you've had it.

Locking competitors out of application file formats was one of the motivations for TCPA: see a post by Lucky Green, and go to his talk at Def Con to hear more. It's a tactic that's spreading beyond the computer world. Congress is getting upset at carmakers using data format lockout to stop their customers getting repairs done at independent dealers. And the Microsoft folk say they want Palladium everywhere, even in your watch. The economic consequences for independent businesses everywhere could be significant.

15. Can't TCPA be broken?

The early versions will be vulnerable to anyone with the tools and patience to crack the hardware (e.g., get clear data on the bus between the CPU and the Fritz chip). However, from phase 2, the Fritz chip will disappear inside the main processor - let's call it the 'Hexium' - and things will get a lot harder. Really serious, well funded opponents will still be able to crack it. However, it's likely to go on getting more difficult and expensive.

Also, in many countries, cracking Fritz will be illegal. In the USA the Digital Millennium Copyright Act already does this, while in the EU the situation may vary from one country to another, depending on the way national regulations implement the EU Copyright Directive.

Also, in many products, compatibility control is already being mixed quite deliberately with copyright control. The Sony Playstation's authentication chips also contain the encryption algorithm for DVD, so that reverse engineers can be accused of circumventing a copyright protection mechanism and hounded under the Digital Millennium Copyright Act. The situation is likely to be messy - and that will favour large firms with big legal budgets.

16. What's the overall economic effect likely to be?

The content industries may gain a bit from cutting music copying - expect Sir Michael Jagger to get very slightly richer. But I expect the most significant economic effect will be to strengthen the position of incumbents in information goods and services markets at the expense of new entrants. This may mean a rise in the market cap of firms like Intel, Microsoft and IBM - but at the expense of innovation and growth generally. Eric von Hippel documents how most of the innovations that spur economic growth are not anticipated by the manufacturers of the platforms on which they are based; and technological change in the IT goods and services markets is usually cumulative. Giving incumbents new ways to make life harder for people trying to develop novel uses for their products will create all sorts of traps and perverse incentives.

The huge centralisation of economic power that TCPA / Palladium represents will favour large companies over small ones; there will be similar effects as Palladium applications enable large companies to capture more of the spillover from their economic activities, as with the car companies forcing car-owners to have their maintenance done at authorised dealerships. As most employment growth occurs in the small to medium business sector, this could have consequences for jobs.

There may also be distinct regional effects. For example, many years of government sponsorship have made Europe's smartcard industry strong, at the cost of crowding out other technological innovation in the region. Senior industry people to whom I have spoken anticipate that once the second phase of TCPA puts the Fritz functionality in the main processor, this will hammer smartcard sales. A number of TCPA company insiders have admitted to me that displacing smartcards from the authentication token market is one of their business goals. Many of the functions that smartcard makers want you to do with a card will instead be done in the Fritz chips of your laptop, your PDA and your mobile phone. If this industry is killed off by TCPA, Europe could be a significant net loser. Other large sections of the information security industry may also become casualties.

17. Who else will lose?

There will be many places where existing business processes break down in ways that allow copyright owners to extract new rents. For example, I recently applied for planning permission to turn some agricultural land that we own into garden; to do this, we needed to supply our local government with six copies of a 1:1250 map of the field. In the old days, everyone just got a map from the local library and photocopied it. Now, the maps are on a server in the library, with copyright control, and you can get a maximum of four copies of any one sheet. For an individual, that's easy enough to circumvent: buy four copies today and send a friend along tomorrow for the extra two. But businesses that use a lot of maps will end up paying more money to the map companies. This may be a small problem; mutiply it a thousandfold to get some idea of the effect on the overall economy. The net transfers of income and wealth are likely, once more, to be from small firms to large and from new firms to old.

This may hopefully cause political resistance. One well-known UK lawyer said that copyright law is only tolerated because it is not enforced against the vast majority of petty infringers. And there will be some particularly high-profile hard-luck cases. I understand that copyright regulations due out later this year in Britain will deprive the blind of the fair-use right to use their screen scraper software to read e-books. Normally, a bureaucratic stupidity like this might not matter much, as people would just ignore it, and the police would not be idiotic enough to prosecute anybody. But if the copyright regulations are enforced by hardware protection mechanisms that are impractical to break, then the blind may lose out seriously. (There are many other marginal groups under similar threat.)

18. Ugh. What else?

TCPA will undermine the General Public License (GPL), under which many free and open source software products are distributed. The GPL is designed to prevent the fruits of communal voluntary labour being hijacked by private companies for profit. Anyone can use and modify software distributed under this licence, but if you distribute a modified copy, you must make it available to the world, together with the source code so that other people can make subsequent modifications of their own.

At least two companies have started work on a TCPA-enhanced version of GNU/linux. This will involve tidying up the code and removing a number of features. To get a certificate from the TCPA corsortium, the sponsor will then have to submit the pruned code to an evaluation lab, together with a mass of documentation showing why various known attacks on the code don't work. (The evaluation is at level E3 - expensive enough to keep out the free software community, yet lax enough for most commercial software vendors to have a chance to get their lousy code through.) Although the modified program will be covered by the GPL, and the source code will be free to everyone, it will not make full use of the TCPA features unless you have a certificate for it that is specific to the Fritz chip on your own machine. That is what will cost you money (if not at first, then eventually).

You will still be free to make modifications to the modified code, but you won't be able to get a certificate that gets you into the TCPA system. Something similar happens with the linux supplied by Sony for the Playstation 2; the console's copy protection mechanisms prevent you from running an altered binary, and from using a number of the hardware features. Even if a philanthropist does a not-for-profit secure GNU/linux, the resulting product would not really be a GPL version of a TCPA operating system, but a proprietary operating system that the philanthropist could give away free. (There is still the question of who would pay for the user certificates.)

People believed that the GPL made it impossible for a company to come along and steal code that was the result of community effort. This helped make people willing to give up their spare time to write free software for the communal benefit. But TCPA changes that. Once the majority of PCs on the market are TCPA-enabled, the GPL won't work as intended. The benefit for Microsoft is not that this will destroy free software directly. The point is this: once people realise that even GPL'led software can be hijacked for commercial purposes, idealistic young programmers will be much less motivated to write free software.

19. I can see that some people will get upset about this.

And there are many other political issues - the transparency of processing of personal data enshrined in the EU data protection directive; the sovereignty issue, of whether copyright regulations will be written by national governments, as at present, or an application developer in Portland or Redmond; whether TCPA will be used by Microsoft as a means of killing off Apache; and whether people will be comfortable about the idea of having their PCs operated, in effect, under remote control – control that could be usurped by courts or government agencies without their knowledge.

20. But hang on, isn't TCPA illegal under antitrust law?

Intel has honed a ‘platform leadership’ strategy, in which they lead industry efforts to develop technologies that will make the PC more useful, such as the PCI bus and USB. Their modus operandi is described in a book by Gawer and Cusumano. Intel sets up a consortium to share the development of the technology, has the founder members put some patents into the pot, publishes a standard, gets some momentum behind it, then licenses it to the industry on the condition that licensees in turn cross-license any interfering patents of their own, at zero cost, to all consortium members.

The positive view of this strategy was that Intel grew the overall market for PCs; the dark side was that they prevented any competitor achieving a dominant position in any technology that might have threatened their dominance of the PC hardware. Thus, Intel could not afford for IBM's microchannel bus to prevail, not just as a competing nexus of the PC platform but also because IBM had no interest in providing the bandwidth needed for the PC to compete with high-end systems. The effect in strategic terms is somewhat similar to the old Roman practice of demolishing all dwellings and cutting down all trees close to their roads or their castles. No competing structure may be allowed near Intel's platform; it must all be levelled into a commons. But a nice, orderly, well-regulated commons: interfaces should be ‘open but not free’.

The consortium approach has evolved into a highly effective way of skirting antitrust law. So far, the authories do not seem to have been worried about such consortia - so long as the standards are open and accessible to all companies. They may need to become slightly more sophisticated.

Of course, if Fritz Hollings manages to get his bill through Congress, then TCPA will become compulsory and the antitrust issue will fall away, at least in America. One may hope that European regulators will have more backbone.

21. When is this going to hit the streets?

It has. The specification was published in 2000. Atmel is already selling a Fritz chip, and although you need to sign a non-disclosure agreement to get a data sheet, you have been able to buy it installed in the IBM Thinkpad series of laptops since May 2002. Some of the existing features in Windows XP and the X-Box are TCPA features: for example, if you change your PC configuration more than a little, you have to reregister all your software with Redmond. Also, since Windows 2000, Microsoft has been working on certifying all device drivers: if you try to load an unsigned driver, XP will complain. There is also growing US government interest in the technical standardisation process. The train is rolling.

The timing of Palladium is less certain. There appears to be a power struggle going on between Microsoft and Intel; Palladium will also run on competing hardware from suppliers such as Wave Systems, and applications written to run on top of vanilla TCPA will need to be rewritten to run on Palladium. This seems a play to ensure that the secure computing platform of the future is controlled by Microsoft alone. It might also be a tactic to deter other companies from trying to develop software platforms based on TCPA. Intel and AMD appear to plan for the second generation of TCPA functionality to be provided in the main processor for free. This might provide higher security, but would enable them to control developments rather than Microsoft.

I do know that the Palladium announcement was brought forward by over a month after I presented a paper at a conference on Open Source Software Economics on the 20th June. This paper criticised TCPA as anticompetitive, as amply confirmed by new revelations since.

22. What's TORA BORA?

This seems to have been an internal Microsoft joke: see the Palladium announcement. The idea is that 'Trusted Operating Root Architecture' (Palladium) will stop the 'Break Once Run Anywhere' attack, by which they mean that pirated content, once unprotected, can be posted to the net and used by anyone.

They seem to have realised since that this joke might be thought to be in bad taste. At a talk I attended on the 10th July at Microsoft Research, the slogan had changed to 'BORE-resistance', where BORE standards for 'Break Once Run Everywhere'. (By the way, the speaker there described copyright watermarking as 'content screening', a term that used to refer to stopping minors seeing pornography: the PR machine is obviously twitching! He also told us that it would not work unless everyone used a trusted operating system. When I asked him whether this meant getting rid of linux he replied that linux users would have to be made to use content screening.)

23. But isn't PC security a good thing?

The question is: security for whom? You might prefer not to have to worry about viruses, but neither TCPA nor Palladium will fix that: viruses exploit the way software applications (such as Microsoft Office and Outlook) use scripting. You might get annoyed by spam, but that won't get fixed either. (Microsoft implies that it will be fixed, by filtering out all unsigned messages - but the spammers will just buy TCPA PCs. You'd be better off using your existing mail client to filter out mail from people you don't know and putting it in a folder you scan briefly once a day.) You might be worried about privacy, but neither TCPA nor Palladium will fix that; almost all privacy violations result from the abuse of authorised access, often obtained by coercing consent. The medical insurance company that requires you to consent to your data being shared with your employer and with anyone else they can sell it to, isn't going to stop just because their PCs are now officially 'secure'. On the contrary, they are likely to sell it even more widely, because computers are now 'trusted'.

Economists have noted that when a manufacturer makes a 'green' product available, it often increases pollution, as people buy green rather than buying less; we may see a security equivalent of this 'social choice trap', as it's called. In addition, by entrenching and expanding monopolies, TCPA will increase the incentives to price discriminate and thus to harvest personal data for profiling.

The most charitable view of TCPA is put forward by a Microsoft researcher: there are some applications in which you want to constrain the user's actions. For example, you want to stop people fiddling with the odometer on a car before they sell it. Similarly, if you want to do DRM on a PC then you need to treat the user as the enemy.

Seen in these terms, TCPA and Palladium do not so much provide security for the user as for the PC vendor, the software supplier, and the content industry. They do not add value for the user, but destroy it. They constrain what you can do with your PC in order to enable application and service vendors to extract more money from you. This is the classic definition of an exploitative cartel - an industry agreement that changes the terms of trade so as to diminish consumer surplus.

No doubt Palladium will be bundled with new features so that the package as a whole appears to add value in the short term, but the long-term economic, social and legal implications require serious thought.

24. So why is this called 'Trusted Computing'? I don't see why I should trust it at all!

It's almost an in-joke. In the US Department of Defense, a 'trusted system or component' is defined as 'one which can break the security policy'. This might seem counter-intuitive at first, but just stop to think about it. The mail guard or firewall that stands between a Secret and a Top Secret system can - if it fails - break the security policy that mail should only ever flow from Secret to Top Secret, but never in the other direction. It is therefore trusted to enforce the information flow policy.

Or take a civilian example: suppose you trust your doctor to keep your medical records private. This means that he has access to your records, so he could leak them to the press if he were careless or malicious. You don't trust me to keep your medical records, because I don't have them; regardless of whether I like you or hate you, I can't do anything to affect your policy that your medical records should be confidential. Your doctor can, though; and the fact that he is in a position to harm you is really what is meant (at a system level) when you say that you trust him. You may have a warm feeling about him, or you may just have to trust him because he is the only doctor on the island where you live; no matter, the DoD definition strips away these fuzzy, emotional aspects of 'trust' (that can confuse people).

Remember during the late 1990s, as people debated government control over cryptography, Al Gore proposed a 'Trusted Third Party' - a service that would keep a copy of your decryption key safe, just in case you (or the FBI, or the NSA) ever needed it. The name was derided as the sort of marketing exercise that saw the Russian colony of East Germany called a 'Democratic Republic'. But it really does chime with DoD thinking. A Trusted Third Party is a third party that can break your security policy.

25. So a 'Trusted Computer' is one that can break my security?

Now you've got it.

This article is reprinted by permission of the author.

Evening talk on MacOS X by David Pogue

Roger Whittaker

On the 10th September a meeting was held at University College London at which David Pogue gave a talk on MacOS X version 10.2 (also known as Jaguar).

David is well known for his books and other writings on Mac OS and for his New York Times column. He was in the UK as a guest of O'Reilly and of MacWorld magazine. The meeting was hosted by UKUUG, and attended by a mixture of UKUUG and London Mac Users Group members.

There were about 100 people present, of whom roughly half identified themselves as Unix users and about half as Mac users.

David described the history of MacOS and the thinking behind the Apple company's move to a Unix-like operating system. In particular he explained the problems of backward compatibility and how previous attempts to replace MacOS had foundered and been abandoned largely because of these problems.

MacOS X solves these problems by being capable of running three types of programs: cocoa, carbonized and classic. Classic programs are those written for previous versions of MacOS which run in what is essentially an emulation mode.

The bulk of the talk focused on the MacOS X GUI: the speaker delighted in putting it through its paces and showing off its 'sexier' features. He also demonstrated the accessibility features including its speech interface, and showed how permissions can be used to restrict particular users to a simple set of applications and features.

David proved to be a very confident and entertaining speaker, and the audience was an appreciative one. It has to be said, however, that some UKUUG members might have liked to hear a little more about the underlying Unix and a little less about the pretty details of the MacOS GUI.

Python Cookbook

Alex Martelli and David Ascher

O'Reilly and Associates

ISBN 0-596-00167-3
606 pp.
£ 28.50

reviewed by John Collins

This book provides a catalogue of techniques for achieving various tasks in Python.

I approached it as a newcomer to Python, although I know an extremely enthusiastic user of the language who had shown me bits of it before. For those who haven't met it before, Python is yet another interpreted language like Perl and JavaScript. It has control structures which actually rely on the indentation of the program to demarcate blocks. It has Object Orientated features nearer to JavaScript than Perl and it has exception handling more like C++. I like Perl, but I have to admit that it is eccentric as the various built-in functions do not have consistent interfaces which I continually have to check up. Python is much more consistent. However I'm a bit of a fan of Perl's "unless" and "until" as alternatives to "if" and "while" and similar, along with the mantra "There's more than one way to do it". There's more than one way to do it in Python too, but probably only one really good way.

Except if you need something nearly identical to the examples in this book, you will need to know some basic Python, and I found myself reading the online tutorial at `http://www.python.org` after I had tried to tackle the first few pages. After that the book was easy to understand. I tried many of the more interesting examples (which can be downloaded from the Website given in the preface) on my Linux machine and had some fun adding a few "frills" of my own.

The earlier chapters introduce basic "howtos" and idioms in Python, not quite in the order understandable to an outright beginner (hence the excursion onto the tutorial) before looking in turn at text handling, file handling, object oriented programming and thread and process management.

Next we look at some actual applications, taking in turn systems admin tasks, databases, user interfaces, networking, web programming, and XML handling. Many of the examples, particularly setting up and using sockets and using XML handling functions, looked, I thought, very much neater than the Perl equivalents, but some would say that about all of it.

The book concludes with some more esoteric techniques (debugging only making an appearance here!) and we even have an overview of how to incorporate new C modules into Python. Finally some more complicated algorithms are presented.

All the examples I tried worked fine and were easy to modify. My one grumble might be that two many examples, including the C extensions, were for Windows and not Linux, but they do tell you where to go to get help.

You will need a proper reference manual to go anywhere further and to get started you will need to go to the tutorial and some purists might disdain a book like this but I think people in a hurry to get a job done similar to the ones in this book will find it a handy reference to plunge into the deep end with and learn the language as they go.

John Collins Xi Software Ltd www.xisl.com

Web Security, Privacy and Commerce (2nd edition)

Simson Garfinkel with Gene Spafford

O'Reilly and Associates

ISBN 0-596-00045-6
786 pp.
£ 31.95

reviewed by Andrew Cormack

This second edition of Simson Garfinkel's book on web security and commerce has added Privacy to the title, which indicates a significant change to the content. Privacy, or the lack of it, now seems to be the major press concern about the Internet and as a result seems to be the main reason why people are starting to take network and server security more seriously. The book identifies three groups of people who may have security concerns about the Web - users, service providers and content providers - and has a section for each of them.

The first section, presumably intended for all readers, is an introduction to web and security technology. The first two chapters, on the landscape and architecture of the web, provide a good introduction, however there are then five chapters on cryptography and identification. The information is well presented, but I suspect it will be off-putting, and not particularly relevant, to many of the book's intended readers. In fact some of the information, for example that on PGP and S/MIME, is barely relevant to the web at all. If this were moved to a reference section later in the book then there would be a better chance of readers making it through to the sections of direct interest to them.

It would be a shame if web users did not get as far as their section, as it contains a good and wide-ranging selection of information about protecting their privacy on-line. There is a short description of how much information can be collected by a server during a browsing session; this is followed by behavioural and technical ways in which the user can control this. The book recognises that even though the legal status of personal data is very different in the USA and Europe, individuals have the same concerns wherever in the world they live. Also, as most of us do not restrict our browsing to web sites in our own country, it makes sense to learn to take precautions at the user end rather than relying on the server to do the right thing with our data.

The server section covers all the levels at which a web service can be attacked. Most books on security concentrate on the operating system and server programs, but this one also deals with physical security, the problems of applications and the need to provide reliable network and DNS services for the site. Many of these areas could fill a book on their own so although there are step-by-step instructions for installing digital certificates on Apache and IIS servers, elsewhere the text highlights things to think about rather than providing full details. There is a chapter on what to do if you become a victim of computer crime, but this deals only with the US legal system.

Finally there is a collection of topics likely to be of interest to web content providers, including access control by IP address, password or client certificates, digital payments and, returning to the privacy theme, policies for handling personal data. This notes the existence of a very different data protection regime in Europe, but only describes in detail the voluntary codes and limited statutory protection provided by US law. There are two chapters on filtering software but, since these conclude that attempts to rate content at the server end have largely failed, it would be more useful to cover this from the user perspective.

Web Security, Privacy and Commerce is now a large book, and contains a great deal of useful information. However readers with specific needs may need to expend time, mental and physical effort, as the volume of information has outgrown the original simple structure of the book. This is not helped by a tendency to wander off the topic of the book: the thirty page biography of Vineyard.net would be of great interest to someone setting up a local ISP, but is out of place in this title. The publishers could help by expanding the existing “Organisation of this Book” section to map out paths through the material for particular types of reader, or perhaps by splitting the book into volumes for users and operators.

Designing Large-Scale LANs

Kevin Dooley

O’Reilly and Associates

ISBN 0-596-00150-9
400 pp.
£ **28.50**

reviewed by Raza Rizvi

Written for people who have a grounding in network design already, this book provides a gathering of principles and tips for developing or extending a network. This is therefore not a theoretical academic work (despite the formulae shown on some of the pages!) but a practical set of notes that can be applied over and over again.

A standard introduction on the reasons to have a network leads us to a lengthy but clearly explained chapter on the elements of reliability within the network infrastructure. With network diagrams, it explains where and why redundancy can be used to overcome single points of failure, documenting the causes of such issues along the way.

The next two chapters take up one third of the book and cover a description of the types of design prevalent in today’s networks and the actual technologies used to implement them. The first is a really good build up from star/bus/ring topologies to take into consideration recovery via Spanning Tree and HSRP/VRRP and then onto VLANs and collapsed backbones. The benefits of hierarchical design following the Core/Distribution/Access model are explained and shown together with routing models. VLANs are then revisited to explain how routing can be applied to trunk circuits and the pitfalls to be avoided.

The technologies described cover humble Ethernet (from 10Mb to 10Gb), Token Ring, ATM, the veritable FDDI, and wireless networks. Each subsection is well written with enough information to cater for most circumstances.

One runs a network infrastructure for the benefit of protocols and the author spends time over the next three chapters covering IP, IPX, and routing protocols. Nothing earth-shattering but a competent backgrounder in the relevant areas.

With the network now built for redundancy and prevention of failure, attention turns to efficiency, based mainly on implementing Quality of Service. The penultimate chapter covers network management and how good design works with network management to achieve the goal of network reliability.

Future issues are considered in the final chapter with information on the design considerations for both multicast and IPv6 networks. A glossary and reading list complete the book.

A very readable text with good illustrations, I would recommend this book to general networking practitioners and those with growing networks of their own who want to be aware of the benefits of good design.

Raza Rizvi is Technical Manager at REDNET. He has ruptured his patella tendon and now sits at home surfing the net!

IP Routing

Ravi Malhotra

O'Reilly and Associates

ISBN 0-596-00275-0
240 pp.
£ **24.95**

reviewed by Raza Rizvi

"Help for Network Administrators" the book nonchalantly says on it‘s front cover, and they are not joking. The target market for this is however not strictly a traditional UK network admin, who is probably more inclined to leave things as they are if they are not broken, but rather this is suitable for those who take an active interest in improving the functionality and stability of their own network or those of their customers.

This is another 'dip and select book', one where the chapters have been broken out into bite sized chunks that you digest as and when you need to. The criteria here is routing protocols, a full six pack, featuring RIP, IGRP, EIGRP, RIP v2, OSPF, and BGP-4.

The author has chosen the order of presentation to assist those perhaps who are using the book as the basis of academic or certification study such that each protocol gets slightly more complex as the pages turn.

After an initial chapter which gives you the basic concepts of routing and explains the value and pitfalls of static routing, each chapter follows the same basic format. There is an explanation of the history of the protocol with details of the convergence mechanism (how the protocol detects failure of routing paths), details of subnet support, route summarisation and finally troubleshooting information.

Naturally the chapters get larger as the more complex protocols like OSPF and BGP-4 are discussed. However, in common with most of the O'Reilly books dealing with Cisco routers, the good use of examples and diagrams greatly assists the points being made in the text and even the more complex subject matter is relatively easy to follow. This is not a book covering every minute variant on the configuration of each protocol, nor does it claim to be, but the author has chosen those features likely to be implemented in all but the most unusual of circumstances.

One thing that was missing on my reading was further details on route manipulation, but it all became clear in the last chapter where the author gathered together the common protocol-independent administrative functions such as route filtering, metric weighting and interface specific blocking.

A useful book for those in the networking field or those wishing to migrate between protocols.

Raza Rizvi is Technical Manager at REDNET. He has ruptured his patella tendon and now sits at home surfing the net

---

Web Performance Tuning (2nd edition)

Patrick Killelea

O'Reilly and Associates

ISBN 0-596-00172-X
480 pp.
£ 31.95

reviewed by Joel Smith

The second edition of this book has been "significantly expanded" to include:

New chapters on web site architecture, security, and reliability, as well as their impact on performance.

Detailed discussion of the scalability of Java on multiprocessor servers.

Perl scripts for writing web performance spiders that handle logins, cookies, SSL, and more.

Detailed instructions on how to use the Perl DBI and the open source program gnuplot to generate performance graphs on the fly.

Coverage of rstat, a Unix-based open source utility for gathering performance statistics remotely.

O'Reilly won their excellent reputation through books like this one. It is focused on its topic, clearly written and thankfully assumes a reasonable level of knowledge about operating systems, networking and the operation of the internet. Unlike many other books, Patrick Killelea will quite happily refer readers to other sources if they need further information on such topics. Consequently there is no need to wade through yet another explanation of Class C address ranges, or how to use ftp.

The book starts off with a series of questions which are useful to track down common performance problems, together with quick tips to improve a site's performance. The rest of first section covers performance monitoring and analysis in much more depth and covers such issues as the trade off between performance and security, as well as providing useful scripts for collecting performance data and load testing your site.

There is a heavy reliance on subheadings which are either descriptive or short questions and statements. These give the book quite a fast pace and have the added advantage of being extremely useful when scanning through a chapter. Killelea continually brings the focus of the book back to real world examples and how the different factors will affect the user's experience at the browser. It is important to monitor the actual web performance, and not just the machine-level load.

The second part of the book, "Tuning in Depth", covers all layers of the browsing experience from the browser through the server through Java applications to underlying database systems and examines ways to improve the performance of each layer. Although this is a revised second edition, it is in this section where the age of the book becomes very obvious (the first edition was written in October 1998). I doubt whether anyone will be caught by the UART buffer overruns caused by modems running faster than the serial ports can deal with. If anyone is still running on such old hardware (which was old even in 1998), the chances are that they are already aware of the issues and the solutions. Similarly, the issue of 56k modems not being compatible with the modems of ISPs is probably redundant these days.

The Server Operating System chapter quotes a 1999 survey of internet host operating systems. The age of this survey makes the results fairly meaningless now, but even at that time, the survey only covered slightly over a million hosts. I would dispute the relevance of drawing conclusions from such a survey even if it was current. All it does is give the impression that the book has dated.

Clearly there have been attempts to update the book. Mac OS X is briefly mentioned, but at the same time there is discussion of the problems of 68K code emulation. Since the PowerPC has been the basis of the Macintosh platform since 1994, this seems very dated. Mac OS X is based on Unix, but by mentioning it in two lines whilst leaving all mention of utilities and applications for the platform based around old OS 9 versions gives the (probably correct) impression that the two lines were added in order to have at least mentioned the new operating system. Windows 2000 (never mind Windows XP) does not even get that much of a mention. If you run a Microsoft environment, do not look to this book for advice on tuning your system.

Although there are a lot of useful suggestions for improving the performance of Java based server-side applications, I suspect that anyone seriously interested in this aspect of performance tuning would be better advised to turn towards the wealth of offerings specialising in Java. The same is true of the section on databases. Seven pages is never going to do more than provide a brief overview of the topic, and to be fair, you are pointed towards sources specialising in this topic.

This book still scores highly on the sections which are general in their scope, particularly the new chapters which have been written for this edition. The more specific sections feel dated, and are likely to further age extremely quickly. Overall the book is still a good source for advice on identifying performance bottlenecks and suggesting ways to tune the infrastructure to eliminate them.

Contacts

Charles Curran
Council Chairman; Events; Newsletter
Oxford
Tel: 07973 231 870
charles.curran@ukuug.org

James Youngman
UKUUG Treasurer
Manchester
james.youngman@ukuug.org

Sam Smith
Website
Manchester
sam.smith@ukuug.org

Alasdair Kergon
Events
Reading
alasdair.kergon@ukuug.org

Alain Williams
Watford
alain.williams@ukuug.org

Roger Whittaker
Schools; Newsletter
Borehamwood
roger.whittaker@ukuug.org

Jane Morrison
UKUUG Secretariat
PO Box 37
Buntingford
Herts
SG9 9UQ
Tel: 01763 273 475
Fax: 01763 273 255
office@ukuug.org