

Apple Worldwide Developer Conference Trip Report (June 28-July 2, 2004)

by Lawrence Peng

Directors Office

L-001

Lawrence Livermore National Lab (LLNL)

DISCLAIMER: These notes are the work of the author. They do NOT represent an official position of any LLNL organization.

The QuickTime video stream for the WWDC 2004 keynote is at the following weblinks:

<http://www.apple.com/quicktime/whatson/appleevents/>

<http://stream.apple.akadns.net/>

Apple is now giving sneak peak information at their website regarding the next major OS X release, code-named Tiger.

<http://www.apple.com/macosx/tiger/>

WWDC attendees got a developer preview copy of Tiger. Based only on that beta, it appears that Tiger will require a Mac with a built in Firewire port. This implies that the "Lombard" G3 PowerBook will become legacy. So effectively Tiger will run on the same machines as Panther, except for the Lombard G3 PowerBook.

Official attendance this year was up 17% over WWDC 2003. Developers of all kinds are there, representing 44 countries. Session tracks covered the usual gamut of low level to higher level issues, along with an enterprise track which tried to address issues that are of concern to system and network administrators. This year there were over 200 technical sessions available.

Other items of interest are that Apple Developer Connection (ADC) membership has jumped from about 96K to 452K from March 2001 to June 2004. In 2001, 81% were OSX only developers, and 19% from Unix, Linux, Darwin. In 2004, 66% were OSX only developers, and 34% from Unix, Linux, Darwin

In addition to being available on Mac OS X and other POSIX based platforms (e.g. Linux, Solaris, FreeBSD), Apple is introducing Rendezvous for Windows as a Technology preview release. (<http://developer.apple.com/macosx/rendezvous/>).

XCode developer tools are being revised to version 2, and there is a web link which gives an overview (<http://www.apple.com/macosx/tiger/xcode.html>).

Keynote Address (June 28, 2004)--Steve Jobs

Status updates

First was the Apple Stores. 80 stores over the last 3 years, with 20 million visitors each year. Doing 250 million dollars of 3rd party sales.

Second was the iPod and iTunes Music Store. 70% marketshare of legal downloads, 50% by player units. Now available in Europe in the UK, France, and Germany.

Third was the PowerMac G5. Steve reviewed the recent updates to the G5 desktops, which included dual G5 processors across the board at 1.8, 2 and 2.5 GHz. Apple has the highest front-side bus in the industry at up to 1.25 GHz per processor.

Last year, at WWDC 2003, Steve Jobs projected that the G5 would be at 3 GHz within a year. Obviously, that did not happen. This was attributed to industry-wide problems in achieving the performance gains expected by moving to the 90 nm manufacturing process (vs 130 nm this time last year). Steve noted that the percentage improvement in performance of the G5 has been 25% versus about 12% for Intel style chips (as measured by clockspeed). While not happy with the situation, Steve was upbeat that the rate of performance increase rate surpassed that of Intel.

New displays and software highlights

Apple introduced new 20 and 23 inch digital displays which are now available. A 30 inch version will be available in August. Some highlights of the new displays are:

- 1) the panel enclosure is aluminum (same as the G5).
- 2) USB 2 and Firewire 400 hubs (2 ports/hub) in the back of the display.
- 3) DVI connectors rather than ADC. Recall that ADC was DVI plus USB 1.0.
- 4) The 30 inch display has a maximum resolution of 2560 X 1600 for a total of 4.1 million pixels (77% more than the 23 inch display). Only works in a PowerMac G5 at the moment because the display needs a new PCI-X graphics card to drive it. The card is the Nvidia GeForce 6800 Ultra and will retail for 599 dollars in August.

Panther (OSX v 10.3) is the most successful OS release in Apple's history in terms of units and revenue. Several new apps are being announced (or qualified) for Mac OS X at the conference including some from Borland (Java development tools), Oracle (Oracle 10g), PeopleSoft (certifying all apps on OSX), Quark (Quark Publishing System) and Sun (Java Creator Studio).

Mac OS X has 12 million users today, up from 7 million a year ago, and over 12,000 native apps. Apple is the number one Unix provider in the world in terms of units.

Steve highlighted a few applications and developers.

Microsoft Office 2004 was mentioned. Steve noted that in a recent dinner conversation with Bill Gates, the two CEO's concurred that relations between their two companies has never been better.

Bob Bennett, the General Manager of Alias (www.alias.com) announced that Maya Unlimited is coming Mac OS X in late summer 2004. He noted that 25% of worldwide sales of Maya Complete is to Mac OS X users, and 70% of downloads of Sketchbook Pro are for the Mac version.

Karen Conroe (Director of Brand Development) from UbiSoft (www.ubi.com/US/) gave a first demo of the upcoming game Myst 4: Revelation.

Daniel Haver, CEO of Native Instruments (www.native-instruments.com/), went on stage to demonstrate Guitar Rig. Guitar Rig is a virtual guitar studio application that can also plug into any application that supports Core Audio plugins (e.g. GarageBand). By using a foot pedal, users can dynamically switch between various guitar presets (supplied or custom created).

Aran Anderson, President of Advanced Analytic System Design (www.advanceddesigners.com), showed a program called Orbit. Orbit is an app to simulate unclassified satellite paths around the earth using data from NORAD, NASA, and the United Nations. It was written in 3 months by Anderson with a PowerBook G4 and XCode development tools. A screensaver version called Freefall is in the works.

Introducing OS X Tiger

Steve then moved on to preview Mac OS X 10.4, code-named Tiger. Tiger is the 5th major release of OSX. Tiger will ship in the first half of 2005.

Tiger is to contain more than 150 new features. Some of the new things are:

- 1) Full 64-bit addressing for working with a very large amount of memory
- 2) 64-bit virtual memory
- 3) 64-bit system library
- 4) Concurrent running of 32 and 64-bit applications
- 5) LP64 support in GCC (long pointer support)
- 6) ACL support (access control lists)
- 7) XGrid to be built-in
- 8) Enhanced SMB (improved performance, Finer grained locking, SMB home directories, NTLM v2 support)
- 9) HTML email composition
- 10) TextEdit application to recognize Microsoft Word tables.

Steve highlighted 10 specific items of interest for Tiger:

A) Spotlight: a new way of searching

- 1) recognizes metadata and names within files
- 2) supports standard formats and extensible
- 3) integrated into apps like Finder, Mail, AddressBook and System preferences
- 4) integrated systemwide, via magnifying glass icon in upper right of screen
- 5) save to smart folder in Finder
- 6) SDK (software developer kit) available today

Spotlight appears to be a system-level database API to access relationships between documents and/or content. It looks like the kind of things promised by Microsoft for Longhorn. It is third party extensible so custom document types can be indexed and understood by apps, and lower-level components of the operating system.

Demos were given on Spotlight integration within apps:

First was using the Finder. Instant search results were returned for freeform searches, using much more than simple filename matching. The Spotlight indexing system can read all sorts of metadata, including those specific to individual file formats. In addition, multiple criteria can be specified, results can be categorized and sorted, and the whole searches can be saved as smart folders in the Finder.

Second was using AddressBook. You can do logic-based searches, such as a smart group that contains a list of contacts that have birthdays in the next seven days.

Third was using Mail. Demo was done for searches across 50,000 messages, and searches can be saved as smart mailboxes.

Fourth was using System Preferences. The text search field was used to identify particular settings, and as the list of results was narrowed, preference panes that match the search were visually highlighted. This makes it clear the the API for retrieval of searches gives you a number of options for what to do with the actual results. You can do lot more than just display a list of results. The System Preference demo also showcased the fact that users can type in terms such as "wifi" or "802.11" when they are actually looking for AirPort settings.

As mentioned earlier, Spotlight is a system-wide facility, not just something application specific. A new Spotlight menu (magnifying glass icon) is present in the upper-right corner of the menu bar and provides search capability for any type of indexable resource.

B) H.264

Next generation video from the MPEG group which has been adopted and ratified. Designed to be scalable from cell phones to high definition video.

C) Safari RSS

Major new addition is RSS feeds (Really Simple Syndication)

- 1) RSS and Atom protocol
- 2) Auto detects RSS
- 3) Personal Clipping service so you can collect and store queries as bookmarks

D) Core Image/Core Video

Core Image and Core Video are frameworks which provide advanced image processing capabilities typically used by the larger software companies. What is significant here is that now a single software developer has access to image tools previously only seen in high end programs like Adobe Photoshop.

More than 100 professional 2D and 3D effects are provided by Apple as part of the frameworks. Apple provides an SDK so developers can write plugin units to create more effects.

Like the Core Graphics framework which is part of Quartz Extreme, Core Image and Core Video rest on top of OpenGL. The calculations for the effects are done using the graphics processor on your graphics card. Calculations are done with floating point precision and are layered. The layering of effects allows for real-time and non-destructive editing. All 2D and 3D filters can be applied to either static images or video. The CPU is used as a fallback if the GPU is not up to the task.

Phil Schiller (Apple's Senior VP for Worldwide Marketing) gave a demo using an app called "Fun House". This was an internal app written in one week by a single person. Schiller made the statement that there is a mechanism which dynamically analyzes the filters and the underlying hardware to optimize performance for any given scenario.

It turns out that Core Image and Core Video are the same technologies that originally made their debut in the Apple program called "Motion". "Motion" was first introduced earlier this year at the National Association of Broadcasters convention (www.apple.com/motion).

E) Dot Mac (.Mac)

Steve mentioned that .Mac has over half a million subscribers. For Tiger, the sync service engine of .Mac will be built in. For example if you have multiple Macs running Tiger then .Mac users will have the ability to sync data across all your Macs. A new preference panel is being added to support this, so that .Mac users can pick which files to sync (Address Book, iCal calendars, pictures, music, etc). Apple released a SDK so that developers can employ the sync engine in their own apps for custom data types (which does not require that developers or users have .Mac accounts).

F) Dashboard

Dashboard presents new opportunities for developers. Steve Jobs called it "Expose for widgets". Initially envisioned for applications which you need to quickly access and quickly.

The widgets are constructed utilizing the WebKit framework. Dashboard widgets are actually web pages. A reasonable description of what Dashboard widgets are is given by Dave Hyatt (who is an Apple software engineer who works on WebKit/Safari):

(http://weblogs.mozillazine.org/hyatt/archives/2004_06.html#005876):

"I wanted to blog briefly to clear up what the widgets actually are written in. They are Web pages, plain and simple (with extra features thrown in for added measure). Apple's own web site says "build your own widgets using the JavaScript language", but that's sort of misleading. The widgets are HTML+CSS+JS. They are not some JS-only thing.

In other words, each widget is just a web page, and you have the full power of WebKit behind each one... CSS2, DOM2, JS, HTML, XMLHttpRequest, Flash, QuickTime, Java, etc. I'll have a lot more to say later on, but I thought it important to clear that up right up front, since a lot of people were asking me about it in email and such.

(http://weblogs.mozillazine.org/hyatt/archives/2004_06.html#005887)

Just to prove a point that there are many ways to think about this new feature, here's another take on what Dashboard is. From a browser geek's perspective, the Dashboard is a collection of HTML sidebar panels liberated from the browser window and placed anywhere on your screen. The "Web pages as widgets" concept is really just a logical extension of the Web sidebar panel metaphor fused with Expose.

The concept of small "Web pages as accessories" inside a browser has existed for years.

When activated (default is the F12 key) Dashboard brings all widgets to foreground, and dims the rest of the desktop. Dimmed applications continue to run.

Among the stock widgets are iTunes, Stickies, webcam, clocks, contacts, and calendar. Apple distributed an SDK so developers can create their own widgets. This basically means that the Mac is now a platform for writing client-side Web applications.

Dashboard has fun visual effects due to leveraging the Core Image framework (e.g. oscillating waves when a widget is activated). Another effect was shown by the Clock widget.

Clicking on the Clock reveals a rotating arrow in the lower right corner. Click on the rotating arrow causes the window to rotate 180 degrees to reveal the configuration options. When finished modifying the configuration options, the window rotates back to show the revised Clock. The rotation effect was reminiscent to a Sun 3D desktop technology demo at the Sun Microsystems Network Conference in San Francisco in September 2003. One of the items shown in the Sun demo was notes being written on the back of windows (http://www.sun.com/software/looking_glass/demo.html).

G) Automator

This is a visual scripting application for AppleScript (and shell scripts) and SDK. Users can create interactive and fully automated scripts. Scripts can also be shared. Over 100 actions are built-in, and Automator currently recognizes many Apple core system apps (e.g. iLife, Mail, Safari, iCal, etc.)

Users may select an action category (defined by function or application). The selected function or application shows the available actions, and users then place the desired action into a script workflow. Output from one action can be used as input to the next action, and actions can prompt for user input.

Apple has provided a SDK so third-party developers can enable users to utilize their apps with Automator.

H) iChat AV

The program will use the H.264 codec in Quicktime for improved video quality. The program now allows for audio and video chats with more than one person at a time. For audio chats, you can now have up to 10 additional people. For video chats, you can now have up to 3 additional people.

Steve did a demo of both audio and video chats with three other Apple employees. The video chats employ clever visual effects which allow all members of the chat to be displayed in one window, rather than having 3 new windows being displayed.

OTHER NOTES:

Below are some highlights from some other sessions I attended. As these sessions were not broadcast to the general public, I am keeping the discussion at a higher level.

OSX State of the Union

The presentation was given by Bertrand Serlet, Senior VP of Software Engineering. He began by reviewing the transition of hardware to the PowerPC, and then reviewed the design goals for the OS 9 to OS X transition. Specifically, Apple wanted to utilize open standards, have a strong design, performance, tools, technologies, and have a platform for innovation.

He then reviewed the progress of OS X since its conception since 1998 to today where we have 17 million users with 12K apps. He thanked the developers for their dedication and then committed to no significant API disruptions in the foreseeable future. I interpreted this to mean that bumps like going from the Tioga printing architecture in Cheetah and Puma to CUPS in Jaguar would no longer be the case.

He then talked about the future with Tiger:

1) Data (specifically metadata--which is data about data)

Data now also coming from external devices such as cameras, iPod, etc.). Files from these kinds of devices are loaded with metadata. Searching metadata often results in richer queries.

One approach which Apple rejected:

- a) put everything into a relational database
- b) define schemas
- c) developers must rewrite your apps

Apple's approach is intended to be more evolutionary by having a systemwide metadata store which gets the metadata via an importer API and query API via an enhanced SearchKit API. Document metadata is put into a relational database by the importer API and then applications can use the query API's to run queries.

The advantage here is that documents remain in files, formats are not modified, apps are not modified, and you just add a system service.

In order to store the metadata, Apple is using the lightweight, embedded, open source, and SQL-based SQLite. SQLite will ship as part of Tiger. A framework called Core Data resides on top of SQLite.

2) Synching of data

Data synching was a priority for Tiger. the iSync engine is being made public as Sync Services. In addition the .Mac API is also going public.

3) Leveraging the G5

Furthering using the G5 was a priority, especially for the lower level (non-GUI) portions of the OS. As a result, Tiger has full 64-bit addressing, tools, and system libraries for the kernel. Also leveraging this is the inclusion of XGrid for highly parallel problems.

4) Other

It appears that Apple is finalizing a new API for kernel extensions (kexts). I presume this is the API that Apple will want developers to use in order to make clean 3rd party kexts, rather than rely on undocumented or private hacks.

Safari/Webkit has undergone continual enhancements as well. Notable is that Webkit can now edit HTML besides just rendering. So for items like Dashboard widgets, you could use Safari as a pseudo prototype and development environment since Dashboard widgets are simply web pages built using Webkit.

Enterprise IT State of the Union

The presentation was given by Bud Tribble, Apple VP for Software Technology Technologies.

Tribble began by reviewing the default security settings of the system (no open ports, Filevault, encrypted disk images, etc.). He outlined Apple's recent enterprise grade offerings like XServe RAID, XServe G5, XSan, OS X Server, and ARD 2 (Apple Remote Desktop v2).

Emerging trends/issues seems to be:

- 1) storage
- 2) backup (disk to disk to tape archive seems to be favored at this time)
- 3) cluster computing (architecture trend is mainframe->client/server->cluster)
(e.g., Virginia Tech, Colsa)

Enterprise solutions available

- 1) IBM Lotus clients for OSX (including Workplace)
- 2) PeopleSoft (Safari certification)
- 3) Novell Groupwise (OSX clients)
- 4) Borland--> optimized suite for Java
- 5) Eclipse--> open source IDE for Java
- 6) Java Studio Creator is available for OSX from Sun.
- 7) Oracle 10g on OSX

During WWDC 2004, Oracle representatives gave an overview of their vision of grid computing and Oracle Real Application Clusters. The idea is essentially to coordinate or cluster the use of many small servers to act as one large computer. Oracle sees grids as multi-machines on the same problem, versus breaking up the problem into smaller chunks which get distributed to individual servers. In the context of Oracle, real application clusters refers to all the computer servers in one room in relatively close proximity. Oracle feels that OS X with Xserve is a great fit to this idea.

All demos were done on Mac OS X. They showed a component of Oracle 10g called HTML DB. HTML DB as the name implies is a declarative 100% web based development environment. Other components of Oracle 10g provide the basis for building AS/J2EE applications.

Betas available now (www.oracle.com/macOS), and Oracle plans to release 10g and the JDeveloper Tools around the beginning of September 2004 which coincides with the next release cycle for other platforms.

OSX Server Overview

High availability clustering

2 node active/passive failover, NFS clustering

Notion of failover has been there since Jaguar, but assumed that the customer would do most of the configuration--and it typically required going to the command line, and no sample scripts were readily available. For Tiger, Apple is going to try the approach of addressing those immediate shortcomings.

Apple emphasized that what is not in Tiger is "live" failover, or fileservices on both nodes (due to filelocking issues) although other services could be on both nodes. Also does not have multi-node access to RAID.

Administration

- 1) File system, services, and directory ACL (Access Control List) compatible with Windows XP/2003
- 2) certificate management

Certificate management now has its own tab in Server Settings. You can use the command line if desired. Integrates with certificate authorities. Setup should be better integrated and shareable across various services like Mail, VPN, etc, unlike Panther.

Open Directory 3

- 1) managed network browsing
- 2) storage of acls and schemas
- 3) OU support

- 4) improve scalability, hot backup
- 5) NTLM v2 authentication
- 6) NT migration tools for Windows PDC to Open Directory, user and group accounts

Managed network browsing means that admin can use OS X Server (using Workgroup Manager) to customize the network views that users see. Configurations are kept in Open Directory. No special client configuration is necessary except to point them to the correct directory bindings. Network views can be nested.

Workgroup and Collaboration

- 1) unified file locks across protocols
- 2) backup DC support
- 3) integrate print services better with CUPS
- 4) iChat server for inside a firewall, encrypted, iChat and Jabber clients
- 5) weblog server including user and group weblogs (based on Blogsom)
- 6) client management
- 7) mobile home directories
- 8) software update server for inside a firewall
 - a) conserve bandwidth(proxy/cache)
 - b) mirrors apple software update
 - c) control availability
- 9) networking
 - a) site to site vpn
 - b) gateway setup assistant for vpn, nat, etc
- 10) internet
 - a) mail virus filtering via spam assassin
 - b) mail virtual domains
 - c) QuickTime High Definition streaming
 - d) mail quotas
- 11) HPC support with built-in XGrid 1.0

Additional features:

- 1) 64 bit app support
- 2) support for Ethernet link aggregation (802.3ad compatible switches)

HPC Technology Update

XServe G5 sales to HPC clusters comprise 40% of unit sales.

Typical hardware is the XServe G5 and XServe RAID, running OSX. Interconnects are Gigabit Ethernet, Myrinet, or Infiniband depending on the calculation.

Dave Paulmark of IBM Toronto gave an overview of XL Fortran Advanced Edition. XL Fortran runs primarily on AIX, but also on Linux and OSX. On OSX it is integrated into XCode, command line supported and supports GDB. The runtime is distributable with

your app. Supports Fortran 77/90/95 and partial 2003. Object linkable with gcc, g++, and IBM XL C/C++. Supports OpenMP on OSX as a tech preview at this time.

Communication and middleware is available from a variety of sources. For example:

- 1) MPICH from Argonne
- 2) LAM-MPI from Indiana University
- 3) MPI/Pro from MPI Software Technology
- 4) MacMPI_X and LnxMPI_S from UCLA

Management tools

- 1) Server Monitor, Server Admin, Workgroup Manager
- 2) XGrid (which supports MPI)
- 3) schedulers
- 4) management/monitors

A recent example of custom deployment was given by Dr. John Medeiros, Senior Scientist at COLSA Corporation (Huntsville, Alabama). COLSA is building a new supercluster for the Aviation and Missile Research, Development, and Engineering Center (AMRDEC) of the US Army (http://www.colsa.com/cover_page/news_front/news_details/news_details.htm).

The cluster is called Mach5 (Multiple Advanced Computers for Hypersonics using G5). Cluster interconnects will start with gigabit ethernet since the problem to be solved is more CPU intensive with relatively minimal inter-processor communications. The cluster is expected to be up for production work by late fall 2004.

The cluster utilizes 1,566 dual 2 GHz G5 XServes for a theoretical performance of 25 TF. The total cost is under 6 million dollars. The system consumes 400 kW peak power, and occupies less than 600 square feet floor space. Solicitation to production is less than 6 months, with solicitation to award in less than 3 weeks. Real world performance is anticipated 12-15 TF using the Linpack test.

File system Access Control Lists (ACL)

Benefits:

- 1) flexible expression of privileges
- 2) support XP clients with OSXS
- 3) better OSX fit with Windows networks
- 4) foundation for collaboration and workflow

Concepts:

- 1) ACL is a list of access control entries, both users and group.
- 2) associate multiple users and groups to objects
- 3) more granular permissions
- 4) permissions inheritance

Tiger ACL model is as follows:

- 1) NT semantics
- 2) fine grained NT permissions
- 3) static inheritance
- 4) allow and deny
- 5) Combine traditional Posix with an ACL
 - a) minimize impact of migration
 - b) maximize compatibility
 - c) API starting point based on the draft Posix 1003.1e

Changes to HFS+:

- 1) no reformatting required
- 2) ACL stored in extended attributes field
- 3) for both client and server
- 4) access to NT ACLs
- 5) access to Active Directory

Changes in Samba

- 1) expose ACL in file sharing
- 2) full fidelity to Windows clients

AFP Server

- 1) effective permissions for Panther
- 2) full ACL for Tiger

Support edit of ACL, manage ACL better through OSXS.

Any filesystem which supports extended attributes gets ACLs for free.

Files may have both ACL and Posix permissions.

Group memberships and ACL

- 1) eliminate 16 group limit
- 2) support nested groups
- 3) compatible with legacy software

Authoritative membership is list of GUID (globally unique ID)

- 1) may reference user or groups
- 2) no schema changes by Active Directory

Introducing PDF Kit

Apple is introducing a set of Cocoa classes which were inspired by the WebKit. At this time, the classes are not available to Carbon applications. An example of their usage is in the Tiger version of the Preview app. The classes rest on top of Quartz and CoreFoundation frameworks.

Some built-in capabilities of PDFKit include:

- 1) viewing facing pages
- 2) select text across pages
- 3) PDF input and annotation
- 4) available as an IB palette

Introducing Core Image

(<http://www.apple.com/macosx/tiger/core.html>)

Core Image is a framework for image processing. When applied to dynamic media the API is called Core Video. These functions have typically implemented in proprietary ways by high end software developers, but now smaller developer shops have access to equivalent functionality. With sufficient hardware would allow image processing in real time (process photos, transitions, video, user interface effects, etc).

As I understand it, the API language is Objective-C, but has no intrinsic dependencies of the App Kit framework. Thus the API should be accessible to Carbon apps.

Core Image's architectural model based on a paper titled "Model for Efficient and Flexible Image Computing" by Michael Shantzis of Pixar given at Siggraph 1994. This model is also used by Apple commercial software called Shake.

Core image uses OpenGL like Quartz Extreme. Core image handles all buffer and state management of OpenGL. It normally runs using the video card graphics processor using a full floating point pipeline. A large number of built-in image filters is provided, and developers can extend (or create) filters via Image units.

Current hardware requirements:

- 1) ARB (Architecture Review Board) fragment program capable
- 2) 128 MB VRAM recommended
- 3) for CPU fallback, G4 processors recommended but G3 will work. The API is velocity engine aware.
- 4) for CPU fallback, multiple processors recommended

Introducing XSan

Introduced at NAB in April 2004

SAN file system for OSX, case sensitive, not using ACL's at this time rather based on Posix like Panther. First release coming in August.

Qualification with OSX Tiger to occur closer to Tiger's release time.

64 bit cluster filesystem

- 1) limited to 16 TB/volume with Panther. Expect to remove that limit with Tiger.
- 2) up to 64 concurrent clients directly connected to the SAN.
- 3) no limits on clients connecting via AFP, SMB, etc.
- 4) file level locking

System is Fibre Channel based. No announcements on iSCSI protocol support, and so far no market pressure to support it.

Support for Tiger ACL expected to need a version 2 release. Details of how to support ACL is currently under evaluation.

Pricing expected to be about 500 dollars for the fibre channel card, which includes the cable, 999 dollars per node, and unlimited capacity. Available in Fall 2004, but beta today (apple.com/XSan)

Getting to the Core of Mac OS X with Darwin

This session was for folks who might want to build their own custom versions of Darwin, which is the foundation of OS X. It is not for the casual user.

A few notes of interest:

- 1) Tiger is targeting using GCC 3.5
- 2) The APSL (ApplePublic Source License) is at version 2, and has been approved by the OSI, and recognized as a free software license by FSF (though not GPL).
- 3) Darwin version is currently 7.0.1 (version 7.0 was used in Panther)
- 4) Source code is obtainable from at least two sites:
 - a) www.opensource.apple.com/darwinsource
 - b) www.opendarwin.org
- 5) If you want to build Darwin from source, the suggested minimum is 384 MB RAM and 2 GB disk space.

If you are building a kernel while using a complete OS X system, then you need to watch out for a few things:

- 1) always build as the root user
- 2) the usual work with a backup!
- 3) do NOT override the CF framework. Darwin includes CF Lite, which does NOT work on a full OSX system.
- 4) modify with caution xnu (the kernel), IOKit user and IOKit drivers and families.

Desktop Management Technologies

Apple's overall goals are to provide flexible tools that can support various management policies, that use a model of one-to-many management, and can evolve as technology moves forward. Some of the major challenges today are how to manage wireless and portable computers, how to deal with hybrid infrastructures, and how to manage the constant barrage of new applications.

Tools to discuss:

- 1) ARD 2 (Mac OSX only)
- 2) Workgroup manager
- 3) Mobil Home directories
- 4) System Imaging
- 5) Software update server

ARD 2 (use ARD 1.2.x for OS 8/9)

- 1) iTunes style console
- 2) observer improved (can show 34 machines vs 4)
- 3) build for mobile computers
- 4) embrace open source (screen sharing via VNC protocol for observe and control)
- 5) Cocoa interface, task metaphor, non-modal
- 6) SQL database back-end
- 7) offline reporting
- 8) can send unix tasks

In Panther, you had mobile accounts (cached accounts), but Tiger aims to make the entire home directory mobile. This capability is not in the WWDC Tiger beta.

- 1) mobile solution for portables
- 2) convenient of network storage
- 3) sync services for local to network and vice versa.
- 4) admins should define a policy that makes sense

Software Update Server (not in WWDC beta).

- 1) Proxy/cache server which connects to Apple's servers.
- 2) Internal machines pull from internal software update server.
- 3) bandwidth expensive
- 4) varying policies
- 5) potential frequent updates
- 6) Quality & Assurance testing

System Imaging/NetBoot

- 1) "Network Image Utility" becomes "System Image Utility"
- 2) support directory services
- 3) per cpu directory service binding
- 4) ASR block copy (fast installs)

- 5) model property filtering
- 6) local client settings adjustable

Workgroup Manager

- 1) managed desktop (preferences)
- 2) define for user, groups, and computers
- 3) delivered via Open Directory
- 4) built in since Jaguar
- 5) preference editor for Tiger
 - a) tweak whatever you want
 - b) plist to "be made human readable"
 - c) hidden features
 - d) preference manifest for Tiger
 - e) to be part of application/tool bundles

Inside Directory Services

For Tiger, plans are to support, update and enhance the following:

- 1) LDAP 3
- 2) AD (Active Directory)
- 3) Server suite
- 4) Admin tools
- 5) Support ACLs
- 6) Support managed network
- 7) Enhance local/server authentication

LDAP v3

Trusted Directory option

- 1) optionally bind to LDAP server
- 2) lock down ldap to known clients

AD (improve AD integration)

- 1) full kerberos support via OD admin
- 2) support AD groups for file system ACL
- 3) continue to work with Redmond

OD (Open Directory) Server suite

- 1) target Open LDAP 2.2.7 or later (vs 2.1.22 today)
- 2) latest MIT KDC
- 3) samba PDC upgrade to support BDC (backup domain controller) functions
- 4) 10.2 and 10.3 clients should continue to work

Open LDAP changes

Directory based schema and access controls

- 1) changes back to OpenLDAP project
- 2) changes posted to Darwin
- 3) expose support for LDAP org unit
- 4) single ldap to server multiple user and group sets

With the changes that needed for Open Directory 3, you cannot mix Panther servers master/replica with Tiger servers. From the standpoint of the client however: Tiger clients can use Panther servers, and Panther clients can use Tiger servers

Server Admin tools

Workgroup manager

- 1) gui based import
- 2) search/apply, simplify batch changes to large set of records
- 3) new cli tools for creating group records "dseditgroup" available today
- 4) one click restore/backup of all directory data to encrypted disk image (so you move it to wherever you want.)

Filesystem ACL support

- 1) filesystem will use 128 bit GUID for filesystem ACL
- 2) new group schema based on GUID
- 3) part of Tiger server

Managed Networks

- 1) new schema in Open Directory server
- 2) change in server and clients tool to use new data

Support NTLM v2

Support Kerberos for SMB file services

Tiger client offer better support for Kerberos only environment

Reminders:

- 1) SLP will either be retired (or optional) in a future release. Move to Rendezvous.
- 2) networking apps should support Kerberos
- 3) Challenge/response based network authentication methods going away in the future.

Integrating Mac OS X in Heterogeneous Networks

This session was geared more towards system administrators to demonstrate how straightforward it is to integrate Mac OS X into a mixed platform environment.

A few salient points from the session were:

- 1) 37 attributes on Active Directory to modify to manage everything via Workgroup Manager.

- 2) OSX as a PDC for NT style services. If have 400 to 600 concurrent Windows PC connections, consider OSX as a PDC. DAS Technology and Versora have NT to OSX migration solutions.
- 3) Migrating to Open Directory from 3rd party LDAP (up to 100K users). You can use standard LDIF import/export CLI tools, or you can use Workgroup Manager. To configure client for both directories using Directory Access.
- 4) Suggest OD (Open Directory) if not absolutely committed to Active Directory.

Safari in the Enterprise

Apple created Safari for a variety of reasons. First, it was considered too important to leave to others. Second, was to support customer and developer communities while adding innovative features. Third, not all Internet Explorer's are equal.

Using WebKit and WebCore, Safari is very standards compliant. However, Apple does have to deal with the current reality of the web in supporting some web extensions which are proprietary. In the future the intent is to focus on consumer sites and enterprise apps, and continue to increase compatibility and performance.

Apple general suggestions for developers is to:

- 1) design to standards (W3C)
- 2) ensure HTML is well formed. Faster and less fragile
- 3) ensure pages include a doctype
- 4) validate static and generated pages at validator.w3c.org
- 5) be browser agnostic

Mark Cianca of the University of California, Santa Cruz discussed using Safari from a customer perspective/requirements. Cianca is the Director of Academic Information Systems, UC Santa Cruz.

Cianca reviewed the UC Santa Cruz migration to PeopleSoft ERP Suite and Cognos BI Suite. The planning process began in late 2001, and is expected to be completed in 3rd quarter 2004. UC Santa Cruz wants their apps to be platform independent, good perceived speed, and minimal to no deployment costs

UC Santa Cruz platform mix for administration tasks is 57% Mac, 41% Windows, with Linux making up the remainder. For all machines on campus, their platform mix to be 41% Mac, 43% Windows, 13% Unix/Linux, and 3% all others.

Cianca described the upgrade process as involving defining business objectives and needs while engaging the vendors. **UC Santa Cruz has adopted the requirement that all vendor demos be given using a Mac.** The assumption is that you can already do it on a Wintel box.

Discovering Quartz Composer

New developer tool for Tiger

- 1) visual programming tool to render/process graphical data
- 2) integrates OpenGL, Quartz 2D, Core Image, Core Video, etc.

Quartz composer core units called "patches"

- 1) analogous to base processing units
- 2) patches can have "input ports", and results to "output ports"
- 3) inputs/outputs can be files, values, or objects
- 4) patches can be aggregated and nested (into macro patches and hierarchical)

Consumer Patches

- 1) render something
- 2) run every frame
- 3) execute in defined order
- 4) pull data

Processor

- 1) run on demand and if inputs change
- 2) process data

Provider

- 1) provide data from outside sources
- 2) run on demand

Quartz Composer projects call compositions. To play compositions

- 1) Use QCView in IB
- 2) binding use QCPatchController (Cocoa bindings)
- 3) Use QCRenderer class (will have to write code, for example to integrate with existing OpenGL code.

Building Interactive Compositions

- 1) interact with external sources like mouse, MIDI, videocams, RSS feeds, etc.
- 2) exportable to DV (but transparency not preserved at this time)

Composer file format is private for now. There were requests to open it up, but no comment on making it public at this time.

File sizes of compositions are reasonably small. Movie files are linked, not embedded. Most movie info is just descriptive info.

With underlying changes made to support the Quartz Composer, the tool technology is not likely to be ported to Jaguar and Panther. If not using anything Tiger specific, then compositions should run fine on earlier systems.

Security Best Practices using Open Source Tools

This session outlined some general do's and don'ts regarding security, and noted some useful open source tools available.

Apple's approach is that admin is admin, user is user, and enable as little as needed. On OS X client, no open ports by default. On OS X Server, only ports 22, 311, 389, 625, 687, and 748 are open by default. All other closed.

Application protocols suggested to use:

OpenSSL to provides certificate management for encryption, authentication and data integrity. New tools should consider using CDSA (which are open source)

OpenSSH to replace things like ftp, telnet

IP firewall is absolutely useful when in an external networks

Kerberos which is a 3rd party key agreement protocol, based on shared keys

Keychains

- 1) central repository for secrets
- 2) X.509 anchors

Password policies:

- 1) server admin/OD can be used to set policies
- 2) password generators
- 3) admin password policies

Network scanners and monitoring (be sure to secure the results!)

- 1) nmap
 - a) life cycle of a port
 - b) quick and dirty scan for ports
 - c) look for near invisible vulnerabilities
- 2) nessus
 - a) actively sweeps network for vulnerabilities
 - b) plug in approach to manage what to scan
- 3) OS-SIM
 - a) listens to all network resources to draw larger picture
 - b) tries to learn what is normal for system

Scan the filesystem (evidence of intrusion can often be in the filesystem)

- 1) tripwire (checksums every file and notes differences)
- 2) Radmin
 - a) think client/server tripwire
 - b) first configure server to hold loadsets from clients

Network Intrusion Detection via SNORT

- 1) another pair of eyes
- 2) hackers do not sleep (10 p.m. to 4 a.m. timeframe is favored)
- 3) uses preprocessor and rules to detect suspicious packets.

HenWen

- 1) OSX front end to SNORT
- 2) easy SPADE configuration
- 3) evaluates suspicious packets via a scoring method (higher score is worse)

Definite Don'ts

- 1) enable "r" utilities (rsh, rcp, etc)
- 2) telnet
- 3) finger
- 4) non-SSL mail protocols
- 5) ftp (use sftp or ssh)
- 6) minimize use of tftp
- 7) non-OD based authentication

You can also always build your own tools!

Summary

As always, the notes above represent only a sampling of the sessions that were available.

Apple has released a various supplemental materials for various WWDC 2004 sessions on the Apple Developer Connection website. The supplemental materials (which vary depending on the session) include documentation pointers, sample code, and release notes.

In order to view them, you need to be able to log into Apple Developer Connection (can get there via Apple's website). The one caveat which I have not been able to test is whether you need to be a paid developer member (meaning Select or Premiere status) or whether just being an online member is good enough.