# Windows Vista Content Protection

Threat-modelling the attempt to seal an open architecture

Peter Gutmann

University of Auckland

## Overview

### What is it?

- Intent of Vista's content-protection measures
- (Brief) Coverage of the technical mechanisms

### Problems

- Some of the ways that it can go wrong

### Analysis

- Effects on the industry
- Inside look at Microsoft politics: Why they did it

### Closing thoughts

## A Note on Sources…

Content-protection details were taken from a variety of sources

- See `http://www.cs.auckland.ac.nz/~pgut001/pubs/vista_cost.html` (now rather out of date) for a few other references and technical information

Best Microsoft reference is "Output Content Protection and Windows Vista" from WHDC

- Otherwise unattributed supporting quotes are taken from various Microsoft documents

Best third-party comment, from ATI, is "Digital Media Content Protection" from WinHEC

## A Note on Sources… (ctd)

Other information was gathered from as wide a range of sources as (practically) feasible

- Hardware review sites, web forums, news articles, blogs, …

  An experiment with a sample size of one is worthless; it may be trivially invalidated by a second experiment that returns the opposite result

  — Introduction to Statistics

Updates, corrections, and further information from readers welcomed

## Updates…

Updated slightly based on feedback from attendees

- Split content across numerous slides to improve readability (several people complained about too much being crammed onto each slide)
- Added several slides covering events like the Atsiv driver and its revocation and Purple Pill, which occurred after the talk
- Added a few slides discussing hardware polyculture effects
- Removed a few slides on DRM politics, a topic that's been done to death elsewhere (see the footnotes slide for more)
- Included a number of extra illustrations
- Some comments and cartoons in here are explicitly meant as jokes/satire to lighten up a long technical presentation. It's a bit sad that I'd even need to add a note to point this out…

## What is It?

## Vista Content Protection

Offspring of ongoing development in Windows XP and remnants of Palladium/NGSCB/etc

- Evolution of XP mechanisms provide the content protection
- Offshoots of Palladium/etc and other OS security research work provide the protection mechanisms

Attempt to turn a general-purpose PC into a sealed audio/video jukebox

> This would turn the PC into a record player as far as music is concerned
>
> — Microsoft Research News

- Direct opposite of the historically open PC architecture

## Content Protection Mechanisms

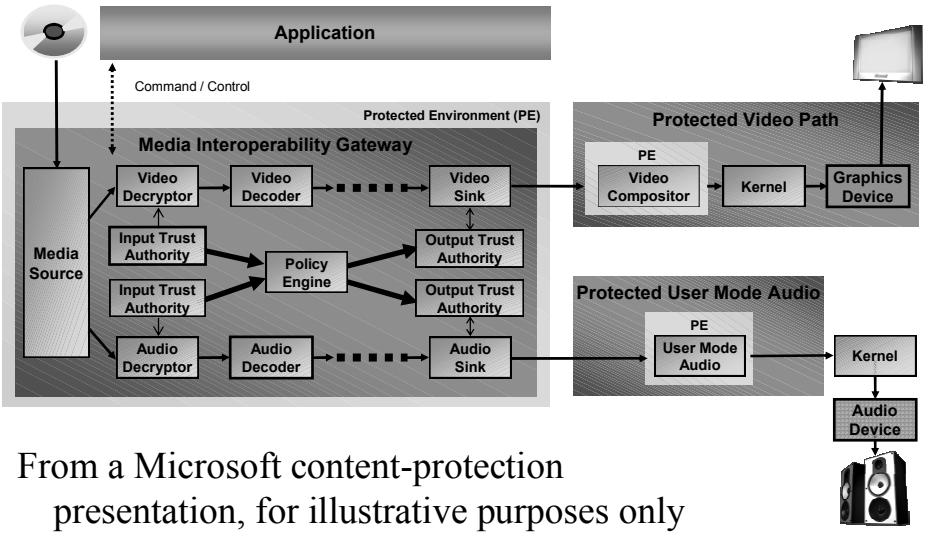
End-to-end encryption of all content paths

- (HD)TV/HD-DVD/Blu-Ray/Internet server ⇒
  (HD drive) ⇒
  decoder ⇒
  renderer ⇒
  display

Content-processing software is protected by OS mechanisms

- Any break in the chain results in degraded (in theory) or no (in practice) output

# Content Protection Mechanisms (ctd)




From a Microsoft content-protection presentation, for illustrative purposes only

# Hardware Content Protection Measures

No unencrypted data on exposed ("user-accessible") buses

- PCI/PCIe
- AGP
- DVI

Buses must be encrypted

— or —

Everything must be integrated into a single device (that doesn't expose a bus)

## Hardware Content Protection Measures (ctd)

Insufficient CPU power available to perform decompression, rendering, and video stream encryption

- Hardware must have video rendering support

End-to-end encryption support in hardware

- Bus encryption requirement means that sound, graphics cards need to have built-in crypto
  - Diffie-Hellman key exchange, AES stream encryption

## Hardware Content Protection Measures (ctd)

Protection against device emulators

- Standard low-tech piracy technique: Grab the rendered video/audio stream
  - Codecs, renderers, etc exist for this purpose
- Countermeasure: Exercise undocumented functionality of the target hardware to check that it's the real thing and not an emulator (HFS)

# Software Content Protection Measures

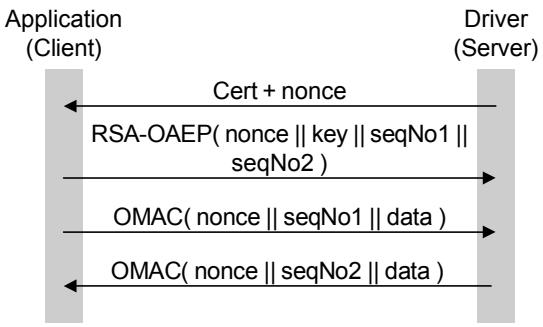
No third-party code where it can interfere with playback operations

- All drivers must be signed in the presence of premium content (or in general for x86-64)
- Drivers are required to incorporate special robustness measures, obfuscation, stealth-virus-like defence mechanisms, …

# Software Content Protection Measures (ctd)

Data *and control channels* are encrypted/MACd

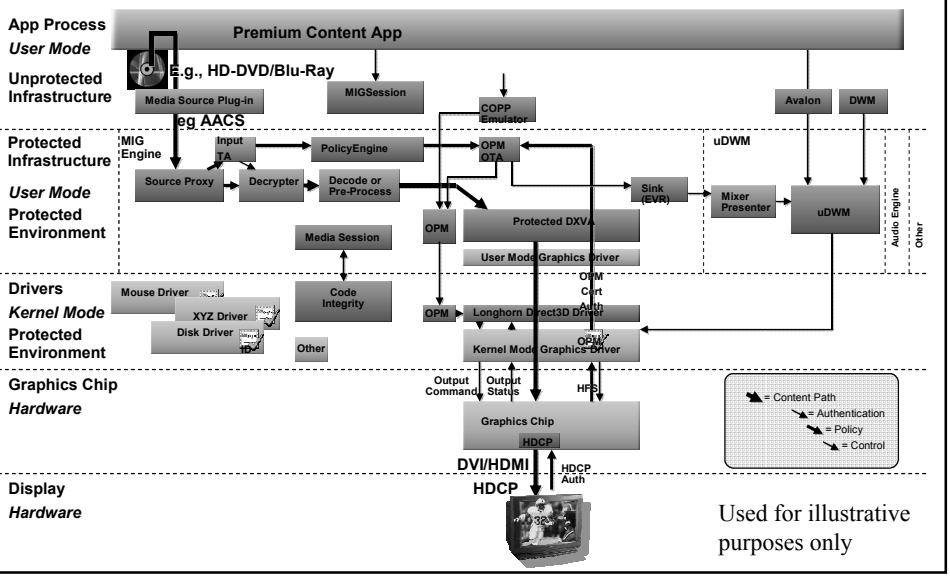
- API calls are run over an SSL-like protocol




- This is *SSL* running between two software components on a PC!

# Software Content Protection Measures (ctd)

In practice it's a bit more complicated than that…




Used for illustrative purposes only

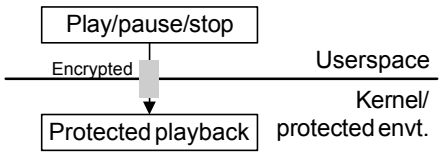
# Software Content Protection Measures (ctd)

Driver certificate provided to the client during the handshake tells the caller what the driver is allowed to handle

- COPP = WinXP mechanism
  - Certified Output Protection Protocol
- OPM = Vista mechanism
  - Output Protection Management
- UAB = Device has a user-accessible bus

# Software Content Protection Measures (ctd)

Playback applications are reduced to being secure remote controls for in-kernel or pseudo-kernel mechanisms




In Windows Vista the application is a remote control for the Media Interoperability Gateway (MIG) environment

- Protected-playback code and data is safeguarded by specialised security mechanisms

# Problems

## Problems

These slides are best read to the sound of an Alka-Seltzer fizzing in a glass…

What Microsoft is trying to achieve here is more or less physically impossible

> Trying to make digital files uncopyable is like trying to make water not wet
> — Bruce Schneier

It's hard enough for a sealed-box DVD player; a hopeless task for the open PC architecture

> The PC industry is committed to providing content protection on the PC, but nothing comes for free. These costs are passed on to the consumer
> — ATI

## Problems (ctd)

This results in some very weird technical requirements

> It is recommended that a graphics manufacturer go beyond the strict letter of the specification and provide additional content-protection features, because this demonstrates their strong intent to protect premium content

Since you can't write technical specs for an impossible task, the best you can do is require that participants show appropriate dedication to the cause

## Problems (ctd)

It must have given the technical writers fits to churn out this stuff

- Imagine trying to write compliance tests for "demonstrate strong intent"

Demonstrating team spirit works for pep rallies, not technical specifications

## Problems (ctd)

Anything that doesn't fit exactly into the Vista content-protection weltanschauung is in trouble

- No-one's quite sure what the rules are, but if you break them you're in trouble

  We've taken on more legal costs in copyright protection in the last six to eight months than we have in any previous engagement. Each legal contract sets a new precedent, and each new one builds on the previous one

  — ATI

  By any standard, Vista's new DRM capabilities hardly qualify as a selling point; after all, it's hard to sing the praises of technology designed to make life harder for its users

  — Matt McKenzie, Computerworld

## Disabling of Functionality

Content can only be sent over protected interfaces

Standard high-end audio interface is S/PDIF (Sony/Philips Digital Interface Format)

- Available as coax digital or TOSlink digital optical output
- Even cheap all-in-one motherboards now feature this
  - Azalea HD audio is a standard feature of Intel chipsets
  - Similar features are available from other vendors

## Disabling of Functionality (ctd)

Since S/PDIF isn't a protected output, it's disabled

> Much of the protection for audio will have to come from turning off various audio outputs

- Result: Premium content → premium silence

Vista prevents your HD audio interface from playing (premium) HD audio!

> Protected audio content is definitely protected. You can't play DRM-protected content over S/PDIF because that would give you a zero-degradation copy that you can do whatever you like with
>
> — Matthew van Eerde, MSDN

> The "disable S/PDIF" behavior is UNCHANGED from Windows XP […] If you don't like DRM, don't use it [DRM]
>
> — Larry Osterman, MSDN

## Disabling of Functionality (ctd)

Standard high-end (non-digital) video interface is YPbPr component video

- It's not protected, so it has to be disabled for premium content

  This feature is no longer supported due to the new Protected Video Path Output Content Protection (PVP-OPM) in Windows Vista

  — nVidia driver documentation

  So there you have it. Apparently the output to a second monitor feature of Cineform is not going to work as it relies on the video card to do this

  — Cineform (professional-level HD video production package) support forum

  – Editing is done on the PC monitor which displays timeline, keyframes, …, finished result is shown on external display

## Disabling of Functionality (ctd)

But wait, this isn't commercial HD content being blocked, this is the user's own content!

- Camcorder manufacturers are moving to HD as fast as their marketing guys can push them
- HD isn't "premium" any more, it's "home movies"

  [Vista] refuses to send content through the component output for my plain jane video files. So the content system disables all content through the non protected output. Its listed in the nvida vista driver news that vista's content protection disables this output. Many forum posts, search engine results for problem. Content protection is active in some form, as I can attest. The mere disabling of UNPROTECTED output while playing UNPROTECTED content is proof enough as far as im concerned

  — Kevin Cripe

## Disabling of Functionality (ctd)

But we've all got HDCP-enabled video cards, right?

- Nope. Vendors had left out HDCP keying support to save hardware costs

  None of the AGP or PCI-E graphics cards that you can buy today support HDCP […] If you've just spent $1000 on a pair of Radeon X1900 XT graphics cards expecting to be able to playback HD-DVD or Blu-Ray movies at 1920×1080 resolution in the future, you've just wasted your money […] If you just spent $1500 on a pair of 7800GTX 512MB GPUs expecting to be able to play 1920×1080 HD-DVD or Blu-Ray movies in the future, you've just wasted your money

  — "The Great HDCP Fiasco", firingsquad.com

## Disabling of Functionality (ctd)

Vendors quickly changed the contents of web sites when this became public

- The wayback archive for ATI/nVidia pages makes interesting reading
- ATI were the subjects of a class-action suit

  I can't playback HD because I need to upgrade my 2 (SLI'd) Nvidia Quadro 4500's (~$2000) to a $200 FX7600GT because it supports HDCP. I can't wait till someone cracks this DRM/HDCP/AACS crap

  — "Sy"

## Disabling of Functionality (ctd)

When Sony announced its BluRay drive for PCs, there weren't any PCs available that could play the content

> Since there are currently no PCs for sale offering graphics chips that support HDCP, this isn't yet possible
>
> — "First Blu-ray disc drive won't play Blu-ray movies", CNet.com

Only by mid-2007 did HDCP-enabled cards with PVP-UAB onboard crypto finally started to appear

> The first PVP-UAB compliant graphics cards are expected to be available […] before the end of 2005

- However even the latest "HD-ready" motherboards like the AliveNF7G-HDready only do 720p playback
  - (This will probably change with time, current in mid-2007)

## Disabling of Functionality (ctd)

Monitors also fall afoul of the lack-of-HDCP problem…

- Vendors are moving from 4:3 to widescreen HD LCD monitors
- Cheaper to produce^H^H^H^H^H^Hconsumers want widescreens

Examples: Philips 230WP7NS HD (1900×1200) LCD monitor, HP LP2465 HD monitor, …

- Inputs are DVI-D, DVI-I and/or D-sub
  - Only analog or non-HDCP digital inputs
- You can do almost anything with these HD monitors…
  …except view digital premium HD content on them!

## Indirect Disabling of Functionality

Disabling of functionality extends into many other areas as well

Example: Automatic echo cancellation (AEC)

- Used to prevent sound from speakers or headphones interfering with other microphone input
- Requires a high-quality copy of the signal and lots of sophisticated signal processing to cancel out the fed-back sound as modified by the PC's environment

Can't be applied any more because the content being echo-cancelled might be premium content

- (Attempts to work around this by providing sort-of access to content)

## Indirect Disabling of Functionality (ctd)

According to the Vista specs, the disabling process is supposed to be dynamic

- The more premium content that's present, the more output gets disabled

  The policy that applies to the resulting mix is governed by the audio that has the most restrictive policy
- If the content is intermittent or varies in strength, so does the output

  Mixes are, of course, dynamic. When piece of audio A is faded out [...] the system is now suddenly able to turn the S/PDIF output back on

See later slides for details on what actually happens

## Decreased Playback Quality

Vista specs require that any premium content sent to unprotected high-quality outputs must be degraded

- STATUS_GRAPHICS_OPM_RESOLUTION_TOO_HIGH ("display quality too good"), probably the most bizarre status code ever defined

Microsoft's definition of a high-quality output: 800×600

- (Specs say 520K pixels, which is roughly 800×600)

Absolute minimum requirements for Windows Vista Basic: 800×600

Result: Absolutely everything supported by Vista needs to have content degraded

## Decreased Playback Quality (ctd)

This can strike at any time, without warning

- No indication to the user that Vista is doing this

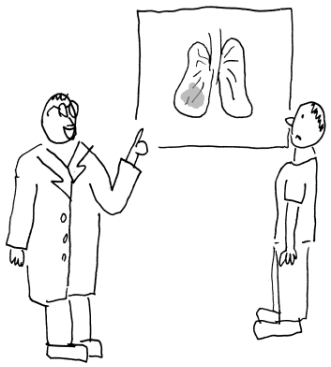


Image courtesy Philip Dorrell

Mr Johnson, that fuzzy region on your X-ray indicates one of two things: Either you have multi-drug resistant tuberculosis, or the copy-protection system on our computer thinks that part of your left lung looks like Mickey Mouse

# Playback in Practice

In practice, degradation isn't an issue

- No known instances of anything actually applying this degradation

In all reported cases in which protection measures have been triggered, content is disabled rather than being degraded


# Playback in Practice (ctd)

Novel attack on computerised security surveillance systems (Karl Siegemund)

- Convince the system that what's being communicated is premium content
- If it's Vista-based, the content will become unavailable

This is tongue-in-cheek, but it demonstrates just how insidious the unintended consequences of this stuff can be

- A bit like the CALEA authors never considering that their ring –1 access to phone communications would be abused by attackers

## Elimination of OSS Hardware Support

Protection against device emulators is implemented via Hardware Functionality Scan (HFS)

- Exercise undocumented functionality of the target hardware to check that it's the real thing

Need to keep device functionality confidential in order to protect the effectiveness of HFS

> The internal workings of the graphics chip must be kept secret, such that a hacker building an emulator could not find out the required information

- If you can write a driver for it, you can write an HFS emulator

## Elimination of OSS Hardware Support

Keeping device internal workings secret locks out open driver support

- Likely that OSS driver support will take precedence over HFS paranoia

In September 2007 AMD started releasing register-level technical specs for ATI GPUs

> So the reason AMD started an open source GPU strategy was purely due to 2 things 1.) Lost CPU sales due to lack of open source GPU support at an OEM level [...]
>
> — David Airlie, phoronix.com

- This would indicate that OSS support does indeed trump HFS

## Elimination of OSS Hardware Support (ctd)

25 years ago, IBM made the momentous decision to make their architecture open

- The entire PC industry is built around this: Anyone can play

This is winding the clock back 25 years to closed, proprietary architectures

> The whole premise of the PC is that it's a UNIVERSAL MACHINE, a machine that can do anything any other machine can do. I have a horrible feeling that Bill may have lost sight of this original vision. If the Vista PC is so hobbled that it can't play the role of a universal machine in the household, then you might as well throw it out the window and just get separate components that do separate functions — i.e. bang goes the PC's raison d'etre
>
> — Peter Stewart

## Problems with Drivers

All of this new functionality presents a nightmare for driver-writers

- Half a year after the OS release, the driver situation is still sufficiently problematic that there's a special web site where people can report drivers that work
- http://ntcompatible.com/compatibility.html

## Problems with Drivers (ctd)

ATI resorted to fudging the Vista certification for their (then) top-of-the-line X1950 graphics cards

- When they finally shipped Vista drivers, they were found to crash the OS on some systems

  I was hit by a BSOD right after the login screen loads [...] Guess what I had to do to get Windows Vista to boot up in normal mode without facing another BSOD? Remove the ATI Radeon X1950 GT and replace it with a non-ATI card

  — "ATI's Vista Killing Driver", techarp.com

  Audio/visual synchronisation became an issue during playback and, laughably, the driver would force a BSOD when entering full-screen mode

  — hexus.net

## Problems with Drivers (ctd)

nVidia followed suit, selling "Certified for Windows Vista" cards without Vista-certified drivers

- A class-action lawsuit followed

Large companies like Dell and Gateway held back on shipping Vista upgrades because they couldn't get drivers

- In April, Dell resorted to bringing back XP for home users
- Microsoft had to release a pseudo-service pack, SP2c, simply to extend the pool of XP product keys for users who were concerned about moving to Vista

## Further Problems with Drivers

HFS requires that vendors create artificial distinctions between product families

- Not just each GPU type, but each stepping of each GPU type
  It is necessary to introduce a chip difference that the HFS mechanism can reliably detect

If stepping X of GPU Y is compromised, the driver for just that stepping must be able to be disabled

- Would result in a re-balkanisation of drivers that have only just completed the long and difficult path to becoming unified drivers
- (Like HFS, vendors are almost certainly "optimising" out this requirement)

## Other Driver Complications

Major design goal of Vista was to get audio/video drivers out of the kernel

- The majority of Windows blue screen issues are due to buggy drivers

Content protection side was trying to push drivers back into the kernel as fast as the kernel developers could move them out

- So a compromise was reached…

## Other Driver Complications (ctd)

Vista introduces a weird SBU level of protection, the protected user-mode process

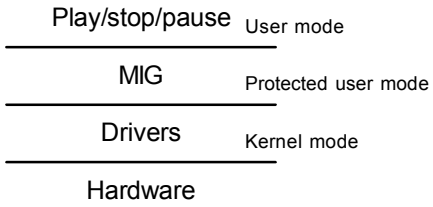
Users are prevented from

- Getting/setting detailed process info
- Changing process ACLs
- Injecting threads (CreateRemoteThread)
- Accessing process memory (Read/WriteProcessMemory)
- Performing control functions on process memory (VirtualAllocEx, VirtualProtextEx, VirtualQueryEx)
- Duplicating handles in processes (DuplicateHandle)
- Performing thread impersonation (for client/server tasks)
- Getting/setting detailed thread info

## Other Driver Complications (ctd)

Essentially this gives admin users only normal-user control over the process

- A peculiar tradeoff between the protection of running in kernel mode and the instability issues of running in kernel mode




Do not attempt to circumvent this restriction by installing a kernel-mode component to access the memory of a protected process

… or Bill gets quite irate?

## User-accessible Buses

Content-protection specs have an obsession with user-accessible buses (UABs)

Drivers must distinguish between a device on the motherboard (no UAB) and one elsewhere (UAB)

- Content can't be provided across a UAB without encryption

## User-accessible Buses (ctd)

How do you tell when a UAB is present?

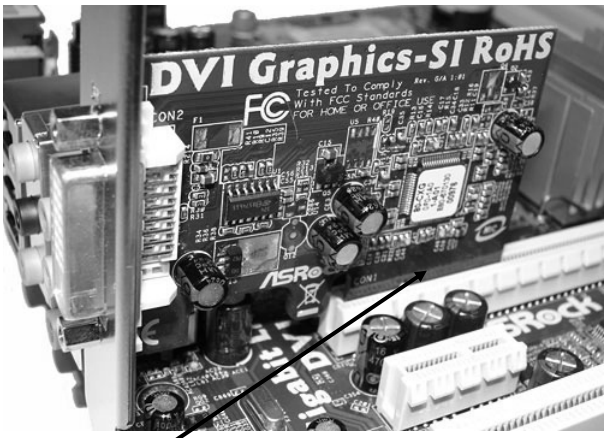
- Device X on the PCIe bus could be on the motherboard or on a plug-in card
- One is a UAB, the other isn't

The specs provide little guidance

> […] it would likely be classed by some content owners as having a user-accessible bus

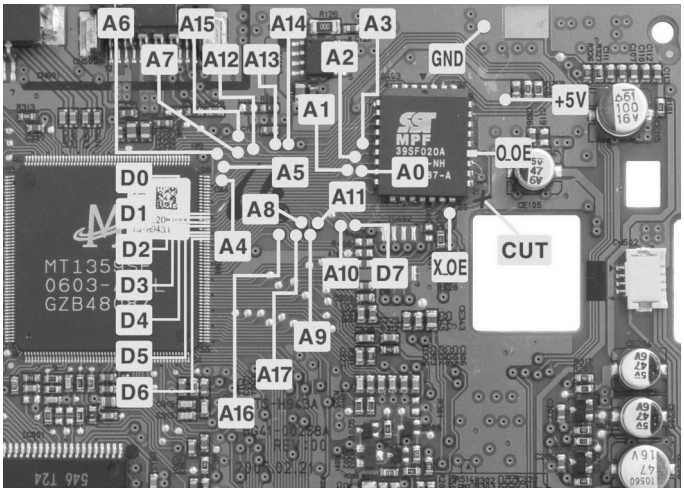
# User-accessible Buses (ctd)

In the case of integrated graphics there is no user-accessible bus, so there is no need for bus encryption and key mechanisms




Is this a user-accessible bus?

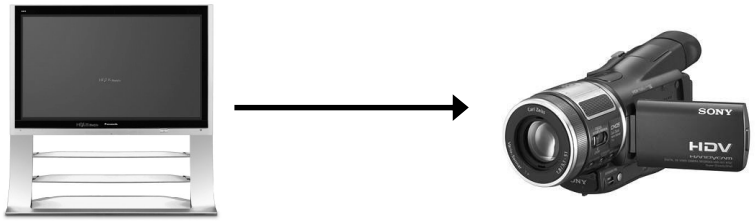
# User-accessible Buses (ctd)




Even this is a user-accessible bus!

# User-accessible Buses (ctd)

The ultimate UAB




- Set up with tripod, perfect lighting, focus → perfect copy

Can control this in cinemas, but will content providers be able to persuade Congress to legislate placing policemen in every living room?

# User-accessible Buses (ctd)

The analog hole again…


- Some high-end sound cards include direct hardware support for this

  These are miniature relays […] which allow the card to record directly from its analog output without using an external loopback cable. Because the Xonar can record at almost exactly the same quality level with which it plays back sound, [this] allows high quality recordings to be made from the card's analog output

  — techgage.com
- (This level of card has seriously overspecced components, the copy quality is perfect)

## Even Further Problems with Drivers

This extends beyond video output

HDMI audio, by design, looks identical to S/PDIF at the hardware and software level

- This was a deliberate design decision to make driver support easier

## Even Further Problems with Drivers (ctd)

The problem is if graphics cards are going to have HDMI connectors, where will graphics cards get the audio from?

A number of vendors redirect the not-OK S/PDIF into the OK HDMI

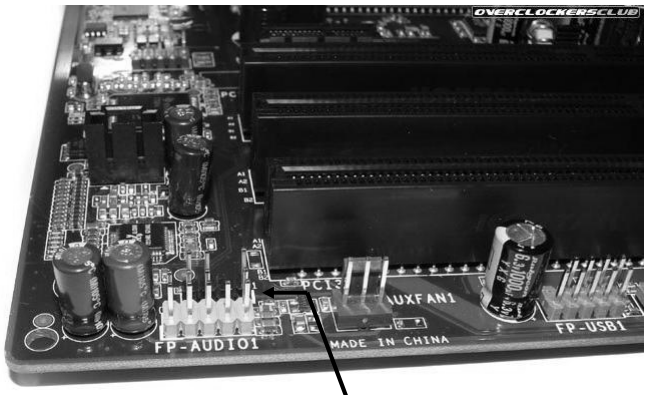
- That's exactly what it was designed for!

But the spec says…

HDMI output cannot be shared with an S/PDIF output under any circumstances. All digital outputs must be independent

- Audio endpoints are supposed to be differentiated using the PKEY_AudioEndpoint_FormFactor property

# Even Further Problems with Drivers (ctd)

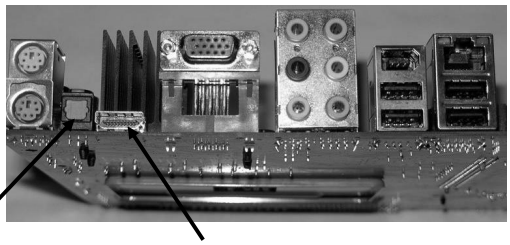



Is this S/PDIF to HDMI audio passthrough allowed?

# Even Further Problems with Drivers (ctd)

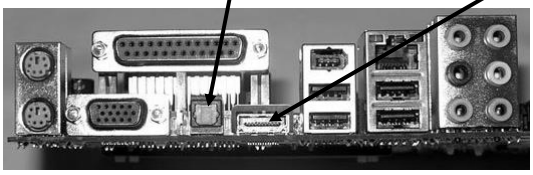
Vista drivers and/or HW vendors are required to implement Maxwell's daemon

Abit all-in-one MB



"Bad" S/PDIF-interface audio out

"Good" S/PDIF-interface audio out



Gigabyte all-in-one MB

## Even Further Problems with Drivers (ctd)

ATI solved this problem by integrating HDMI audio into their video cards

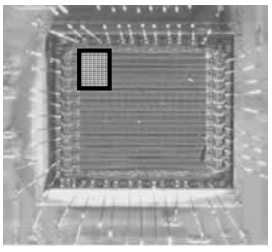
With the advent of HDMI, an interesting PC ecosystem adjustment will happen. Graphics manufacturers will need to get into the audio business

- (Microsoft innovates in the hardware field)

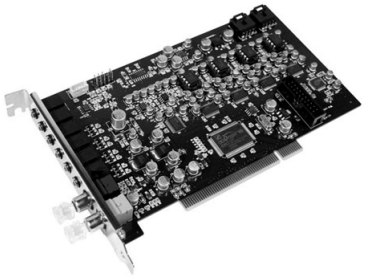
## Even Further Problems with Drivers (ctd)

Probably less than thrilling for people with high-end audio aspirations

- Budget for integrated audio may be 2cm$^2$ and no more than $0.10 BOM increase

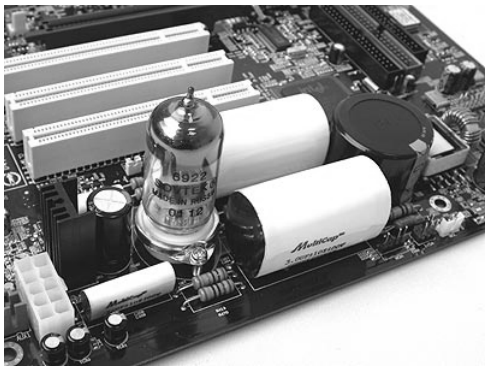


- c.f. audio cards 100cm$^2$ and up to several hundred dollars worth of top-of-the-line components



## Even Further Problems with Drivers (ctd)

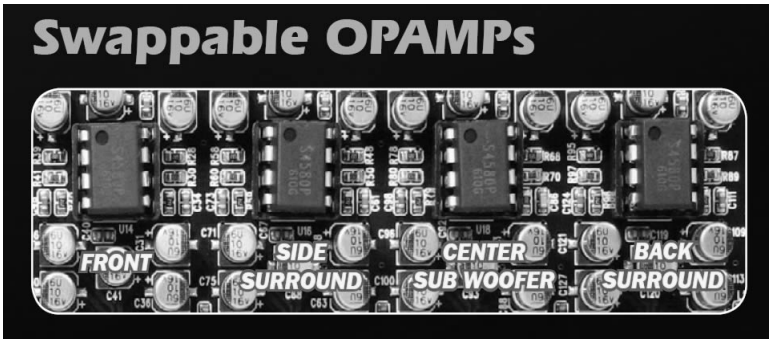
The golden ears crowd and gamers are a tough audience…



- Asrock P4 motherboard

## Even Further Problems with Drivers (ctd)

A *really* tough audience…




- X-Meridian sound card, targeted at serious audio enthusiasts

## Even Further Problems with Drivers (ctd)

Moving sound into the video card can disable onboard sound, since it's not appropriately protected

> We noticed that AMD's [ATI] drivers over-ride motherboard-based audio without prompting, such that novice users may wonder why there's no sound from the audio jacks on the I/O section
>
> — hexus.net


May be just a driver bug, but it demonstrates the problems of requiring physically distinct channels for protected and standard content

- Users who have just set up a 7.1 surround sound system on their PC will probably be less than impressed

## And Even Further Problems

Drivers can potentially interfere with content protection

Solution: Require all (64-bit) drivers to be signed

- (Insert standard shopping list of reasons from ActiveX history for why this doesn't work)

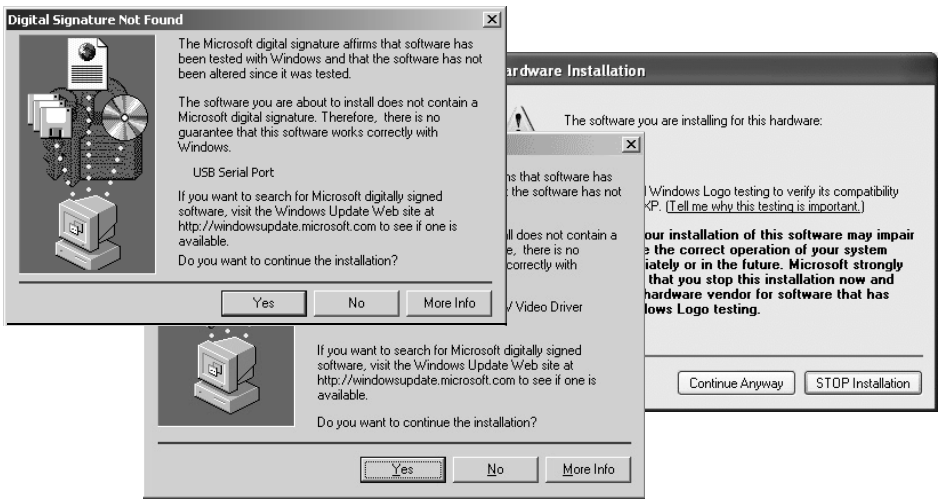
Both the ATI and nVidia drivers contain sufficient bugs to allow an attacker easy kernel-mode access

- You can even include these drivers in your rootkit!

Ah, the wonders of identity-based trust…

# And Even Further Problems (ctd)

The entire PC industry is built on top of masses of (unsigned) third-party drivers




# And Even Further Problems (ctd)

Check the install instructions for any PC hardware you buy that includes drivers

- It's so common that it's even present in computer books and Windows install guides

Effect of the driver-signing requirement on vendors is currently hard to assess due to the paucity of 64-bit drivers

- (Although the paucity of 64-bit drivers could be a direct result of the driver signing requirements)

## And Even Further Problems (ctd)

This makes debugging and in general working with 64-bit device drivers a major pain

- Throwback to the 1980s and DOS driver development
  - Individually customised drivers are particularly nasty
- Need to go into a special operating mode with F8 on boot to allow unsigned driver loads
  - This disables handling of protected content
- Can kludge it with a test signing cert during development
  - Even then you need to boot the machine into a special configuration first (TESTSIGNING ON)

Still doesn't solve the problem for post-development release mode

## And Even Further Problems (ctd)

One driver developer created a signed 64-bit load-anything shim (Atsiv) to fix this problem

- Restores sanity to 64-bit driver development and deployment

  [Atsiv] assists users of Microsoft Vista that are currently unable to use legacy hardware without signed drivers, and casual developers (such as hobbyists) that are not able to use a company's signing certificate

  — Linchpin Labs

  – c.f. GiveIO driver from DDJ, used with Win2K/XP applications to provide device access from user mode

Of course you can use this shim to load *anything*…

## And Even Further Problems (ctd)

Certificate was revoked by Verisign, the code-signing CA

- … but also added to Vista's kernel mode code signing revocation list
- … and blacklisted by Windows Defender
- (Someone *really* didn't like this driver)

They couldn't really explain why

- It didn't seem to violate any documented restrictions

See blog at http://blogs.msdn.com/windowsvistasecurity/-archive/2007/08/03/x64-driver-signing-update.aspx for further extensive discussion from both points of view

## And Even Further Problems (ctd)

Protected User Mode lasted for all of a month before Alex Ionescu figured out how to bypass the special status of protected processes

```
c:\>dpinpurr 312 /p
[C0000156] - STATUS_TOO_MANY_SECRETS:
        Process modified successfully!
c:\>
```

- (312 is the handle of the Protected Media Path process)

## And Even Further Problems (ctd)

Alex later released a program to load anything into the kernel using ATI driver bugs

- Purple Pill utility turns off driver-signing checks
  - Does more or less the same as Atsiv did, but using a signed driver shipped by a large vendor

> It is likely that Microsoft will use its automatic update mechanism in Vista to ship a patch for this buggy driver. The company cannot revoke the certificate for the driver because, as Ionescu explained, it's already embedded in about 50% of all Vista laptops — and any revocation will affect those machines
>
> — ZDNet

## And Even Further Problems (ctd)

This is a *textbook example* of the problems with the thinking behind the content-protection model

> Vista will […] revoke any driver that is found to be leaking premium content […] if the same driver is used for all the manufacturer's chip designs, then a revocation would cause all that company's products to need a new driver
>
> →
>
> The company cannot revoke the certificate for the driver because […] it's already embedded in about 50% of all Vista laptops — and any revocation will affect those machines

Can I say "I toldja so" now?

## Denial-of-Service via Driver Revocation

If a driver is found to be leaking premium content, Microsoft would revoke its right to be fed that content

> Vista will […] revoke any driver that is found to be leaking premium content […] if the same driver is used for all the manufacturer's chip designs, then a revocation would cause all that company's products to need a new driver
>
> This revocation is actually a benefit to the graphics manufacturer, by helping to protect against actions that a content provider might take against that hardware manufacturer in case of leakage

Causes serious problems due to interactions with other aspects of Windows…

- (Not to mention the problems from the previous slide)

## Denial-of-Service via Driver Revocation (ctd)

Downgrades disguised as upgrades provide a strong disincentive to applying service packs/hotfixes

- Malware is invisible to users
- Crippling of functionality isn't

  → Incentivises users to disable Windows updates

## Denial-of-Service via Driver Revocation (ctd)

Windows' anti-piracy component WGA/SPP is strongly tied to system hardware components

- Make too many hardware changes and your Windows license validation is invalidated
- Driver revocation → license invalidation
  - Particularly nasty for e.g. motherboard-integrated video, which leads to automatic license invalidation

In any case this will never work in practice for the reason given earlier

> The company cannot revoke the certificate for the driver because […] it's already embedded in about 50% of all Vista laptops — and any revocation will affect those machines

## Denial-of-Service Tricks

Use an HDCP stripper (sometimes sold as "DVI amplifiers") to make HD output work


- Actually recommended by a Westinghouse VP of Marketing to make Westinghouse HD TVs work with PS3s

  > Purchase an HDMI to DVI adapter to bypass HDCP
  >
  > — Rey Roque, Westinghouse VP of Marketing

Relatively easy to build using COTS devices

## Denial-of-Service Tricks (ctd)

Use an HDMI/HDCP chip employed in vast numbers of consumer electronics devices

If you're feeling really devious, recycle HDMI chips from junked TVs

- Standard practice for TV servicemen when something major like a picture tube or yoke fails
- Components like the jungle IC can cost $50-100 to replace and take weeks or months to source, so it makes sense to recycle these parts

## Denial-of-Service Tricks (ctd)

Content providers have two options

1. Shut down vast numbers of consumer devices
   - Imagine Sony Pictures shutting down Sony Electronics devices
2. Allow HDCP strippers to proliferate unchecked

They really didn't think this one through too well

- (Could probably add that comment to half the slides in this talk)

## Digression: How not to do Sec. Engineering

AACS provides a smorgasbord of keying options

- Many, many keys used for all sorts of purposes at various levels of the system
- Provides a great deal of flexibility…
  … especially if you can control where you want to compromise the system

Attackers get to choose between revealing a blanket-coverage but easily-traceable (and revocable) key or a single-title but untraceable/revocable key

- This highly flexible keying system probably serves the attacker better than it does the defender

## Digression: How not to do Sec. Eng. (ctd)

Read the AACS specs in reverse: To force the defender to perform unpalatable action X, the attacker should do Y

## Digression: How not to do Sec. Eng. (ctd)

Content industry threat model: The only conceivable use for consumer electronics is to pirate content

- Goes back at least to compact cassette recorders and VCRs

  The VCR is to the American film producer and the American public as the Boston strangler is to the woman home alone

  — Jack Valenti, former head of the MPAA


## Digression: How not to do Sec. Eng. (ctd)

Consumer threat model: These guys are p***ing us off, let's do the same thing to them

> With the HD-DVD, I wasn't able to play my movie on my non-HDCP HD monitor. Not being able to play a movie that I have paid for, because some executive in Hollywood decided I cannot, made me mad… I'm just an upset customer
>
> — "muslix64"

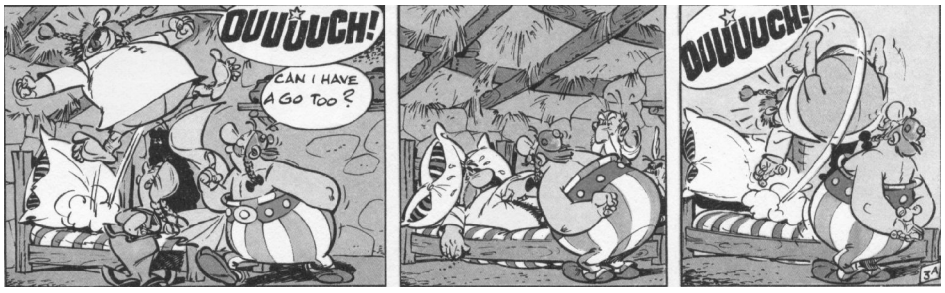
- Consumers now have both the motivation and the means to not necessarily get at the content but to get at the content industry

Destructive interaction between the two threat models

## Digression: How not to do Sec. Eng. (ctd)

You are now a puppet of the attacker

- They get to choose which strings to pull




If you create fortifications with only one way in, remember that there's also only one way out

## Extended Digression: Threat Modelling

Most famous authentication protocol is Needham-Schroeder

- Proposed in 1978, proven secure
- Found to have problems and re-proven using BAN logic
- Still found to have problems but re-proven using FDR
- Still found to have problems using the NRL protocol analyser

Each new analysis discovered flaws in the assumptions made in previous analyses

## Extended Digression: Threat Modelling (ctd)

Example: A principal can impersonate themselves

- Who cares?
- This is about as useful as forging your own signature

What if the principal is two processes running at different privilege levels

- $Me_1$ (user) impersonates $Me_2$ (root)
- In the real world the protocol entity "you" isn't a person but one or more agents acting on your behalf
  - All(?) (non-agent-based) protocols assume that the principal is an atomic entity, and that user ≡ user agent

Suddenly self-impersonation becomes quite useful

## Extended Digression: Threat Modelling (ctd)

Intent of digital signing in conventional thinking

- Protect the content from modification
- Provide endorsement of the content
- Associate the signer with a content
- Prove involvement in the act of signing

  … etc

What if you want to forge your own signature (or at least fool yourself about the validity of your data)?

- Again, who cares?

## Extended Digression: Threat Modelling (ctd)

AACS implements a high-water-mark mechanism to prevent rollback attacks

- Key block containing blacklist entries must have a higher number than any previously-seen key block to be regarded as valid

To immunise a device against ever being revoked, feed it a blacklist with the version number (= generation counter) set to UINT_MAX

- To do this you need to be able to forge a signature on your own (well, licensed/purchased) content

## Extended Digression: Threat Modelling (ctd)

How to do this

- Hook the filesystem read function using any standard hook technique
- Use `VirtualProtect` to make the second 4K (an x86 page) of the read buffer a guard page
- Return control to the caller
- Once the hashing for the signature check gets to the second page, the guard page exception will be triggered
- Move back 4K-8 bytes from the exception location and set the value there to UINT_MAX
- Return control to the caller

## Extended Digression: Threat Modelling (ctd)

You now have a verified digital signature on a media key record with a counter value of UINT_MAX

- Digital signature threat modeling never anticipated a situation where $Me_1$ wants to fool $Me_2$

(A much simpler approach: Patch the code that does the verification as per doom9.org)

## Extended Digression: Threat Modelling (ctd)

Content protection isn't a standard crypto/security problem

> Protocol goals are often formalized as if agents could engage in a protocol run only by following the rules of the protocol
>
> — Dieter Gollman

What might a phisher do when confronted with a [redacted]-protected site?

- Notice that the site has some kind of login protection and immediately move on to an easier target
- Duplicate the site and spend hours writing a program […] ultimately failing
  — Vendor FAQ
- A study of this type of mechanism found that 92% of users fell prey to attackers when the attackers didn't follow the directions in the vendor FAQ

## Extended Digression: Threat Modelling (ctd)

Once the enemy is the user, standard security thinking falls apart

> I propose that each copy of the OS should ship with an orange jumpsuit and sensory deprivation goggles, since all Vista users have been unilaterally declared 'enemy combatants' by the content apparatchiki
>
> — Daniel Nevin

A mass of other ideas on content-protection holes have been passed around by security researchers

- Little public discussion of the issues due to DMCA concerns

## Tilt Bits

The Vista content protection spec requires that hardware and software drivers set "tilt bits" if they detect anything odd

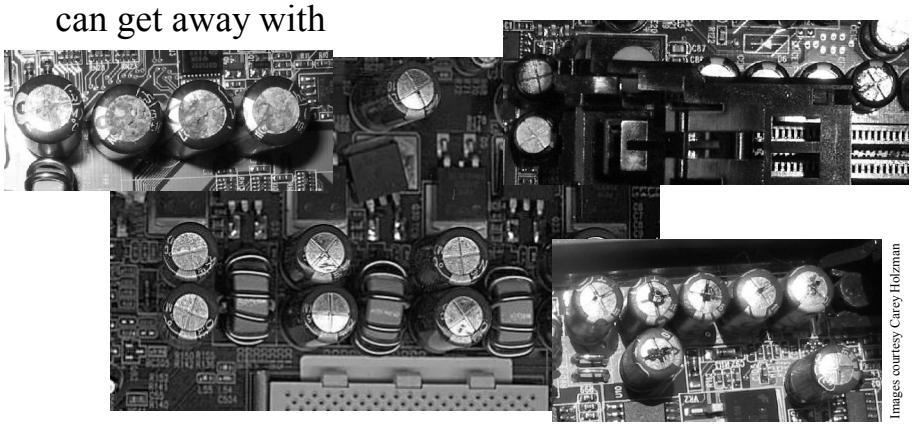
- Jitter on bus signals
- Odd timings for signals
- Device registers with unusual values

…

> The idea [of tilt bits] is basically insane
>
> — Dave Walker

## Tilt Bits (ctd)

PCs are built from the cheapest parts that the manufacturer can get away with



Images courtesy Carey Holzman

Tilt bits mean that otherwise unnoticeable glitches are suddenly surfaced and turned into showstoppers

## Tilt Bits (ctd)

Consider the scenario of a warship operating in a combat zone

- A near-miss scrambles the system bus just enough to activate tilt bits

In September 1997, Windows NT disabled the Aegis missile cruiser USS Yorktown

- In 2007, Windows Vista can do this via a by-design feature of the OS

## Tilt Bits (ctd)

No vendor in their right mind would implement this stuff

- Either "forget" to implement it or fake it

  I can not only say that the idea [of tilt bits] is basically insane, but I can also see hardware manufacturers refusing to implement tilt bits, or more likely, faking their functionality
  — Dave Walker
- (The vagueness of the specs make it easy to fudge this)

## Tilt Bits (ctd)

Faking things is already routinely done for WHQL graphics driver evaluation

- WHQL = safe and slow mode, release = fast and somewhat risky mode
- One common trick: Check for an obscure enable-unsafe-optimisations flag
  - WHQL installer doesn't set the flag on install
  - RTM installer sets the flag on install
- Same (signed) driver, totally different behaviour

## Tilt Bits (ctd)

Try running graphics drivers under Microsoft's Driver Verifier and compare the performance

Try renaming graphics applications/benchmarks and compare the performance

- DirectX Tunnel demo TUNNEL.EXE → FUNNEL.EXE
- quake3.exe → quack3.exe (HardOCP)
- 3DMark03.exe → 3DMurk03.exe (techreport)

This driver duality may explain ATI's certified but Vista-crashing drivers

## Increased Hardware Costs

Control over hardware design issues is passed over to Hollywood

> The evidence [of security] must be presented to Hollywood and other content owners, and they must agree that it provides the required level of security. Written proof from at least three of the major Hollywood studios is required

## Increased Hardware Costs (ctd)

To provide Vista-approved security-related functionality, you need to get well-known security experts like MGM, 20th Century-Fox, and Disney to sign off on it

- Gives a whole new meaning to "Mickey-Mouse security"

  This increases motherboard design costs, increases lead times, and reduces OEM configuration flexibility. This cost is passed on to purchasers of multimedia PCs and may delay availability of high-performance platforms
  — ATI

## Increased Hardware Costs (ctd)

Only certain configurations and board layouts are permitted

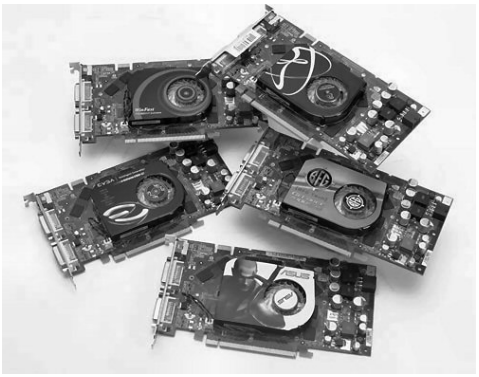
> Cannot go to market until it works to specification… potentially more respins of hardware
> — ATI

Computer design is now dictated not by electronic design rules, physical layout requirements, and thermal issues, but by the wishes of the content industry

## Increased Hardware Costs (ctd)

Standard video-card manufacturing process

- Clone the reference design



- Omit components for different price points

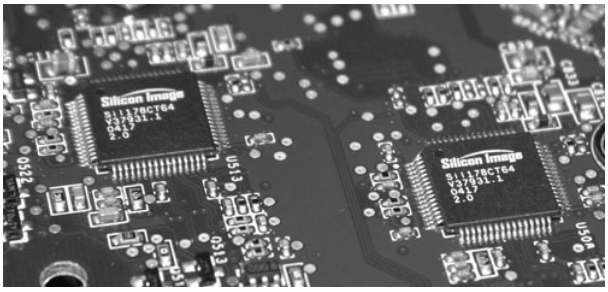
## Increased Hardware Costs (ctd)


Is this a user-accessible bus?

## Increased Hardware Costs (ctd)

In some cases it's more than a price differentiator, it's required for devices to function

- Many GPUs only provide a single TMDS output

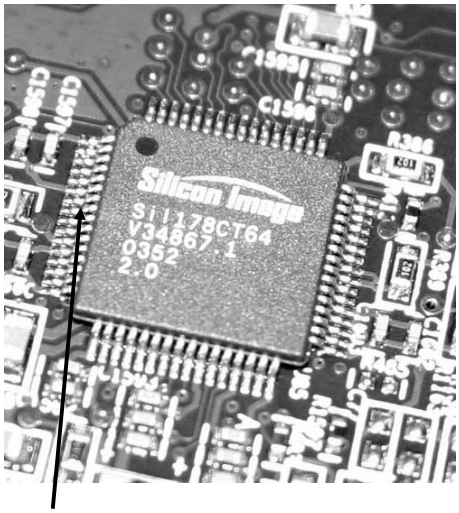



- The second output is provided by a DVO (Digital Video Out) link feeding an external TMDS transmitter

## Increased Hardware Costs (ctd)

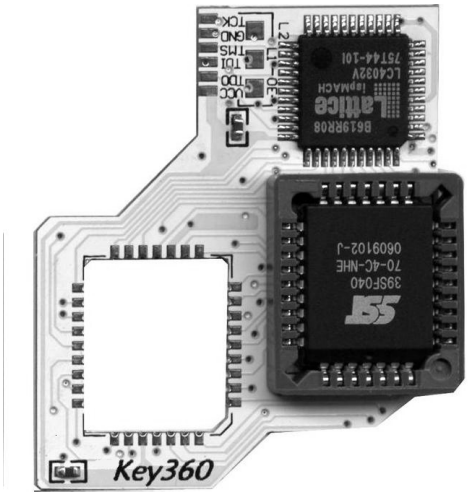
Some high-resolution displays explicitly require multiple DVI/TMDS links because single-channel DVI doesn't have enough bandwidth

## Increased Hardware Costs (ctd)




Is this a user-accessible bus?

## Increased Hardware Costs (ctd)




Are you sure this isn't a user-accessible bus?

## Increased Hardware Costs (ctd)

Intent of content protection is to stop commoditisation of the copying process

Oops

- "We will roll them off the assembly line like sausages"

## Increased Hardware Costs (ctd)

What if a problem is discovered with the design?

> Company shall promptly redesign the affected product […] if such redesign is not possible or practical, cease manufacturing and selling such product

Falls under restraint of trade/antitrust

- Court may find that it was agreed to under duress
- Difficult to determine what the outcome of such a case might be
  - Would also vary on a country-by-country basis
- Severability could help to ensure its survival in the US

## Further Cost Increases

Vendors are required to license third-party IP purely for content-protection reasons

HDCP for HDMI is owned by Intel

> HDCP is the Intel protection scheme for DVI and HDMI […] and must be licensed

- Have to pay Intel royalties even though you can do the same thing for free over DVI

Intel also owns the AES-128 based Cascaded Cipher used to encrypt content

- More unnecessary royalties

## Further Cost Increases (ctd)

Licensing HDCP for HDMI is a nightmare

- ATI/AMDs flagship RS690 (a.k.a. Radeon Xpress 1200) / AMD690 chipset was delayed because of HDCP licensing issues
- AMD has a general HDCP license, but no license for the 690 specifically
  - Users have to pay per-product fees alongside yearly fees
- This licensing issue runs all the way down the food chain

> Although the AMD 690 variants will support HDMI [with HDCP], AMD isn't allowed to mention HDMI support without a license. Specific manufacturers anticipating to announce RS690 motherboards will still need valid licenses for HDMI, HDCP and Macrovision, as well as per-board validation
> — dailytech.com

## Further Cost Increases (ctd)

HDCP comes with a strong built-in disincentive for its use

- Asian manufacturers are building HDMI/HDCP-free products not necessarily to encourage piracy but simply because it's such a royal pain to license and use

Delays development, delays products, reduces interoperability, increases costs

## Further Cost Increases (ctd)

Microsoft have recommended that device vendors license third-party obfuscation toolkits to provide stealth-virus-like cloaking to their code

> Drivers must be extra-robust. Requires additional driver development to isolate and protect sensitive code paths
> — ATI

- Vendors like Cloakware and Arxan have added "robustness solutions" web pages to their sites to cash in on this lucrative market

> [Additional testing and support costs are] potentially the highest cost of all
> — ATI

# Additional CPU Consumption

Content-related communications (i.e. function calls) have to be run over an SSL-style protocol

Drivers are required to poll underlying hardware every 30ms to ensure that everything appears kosher

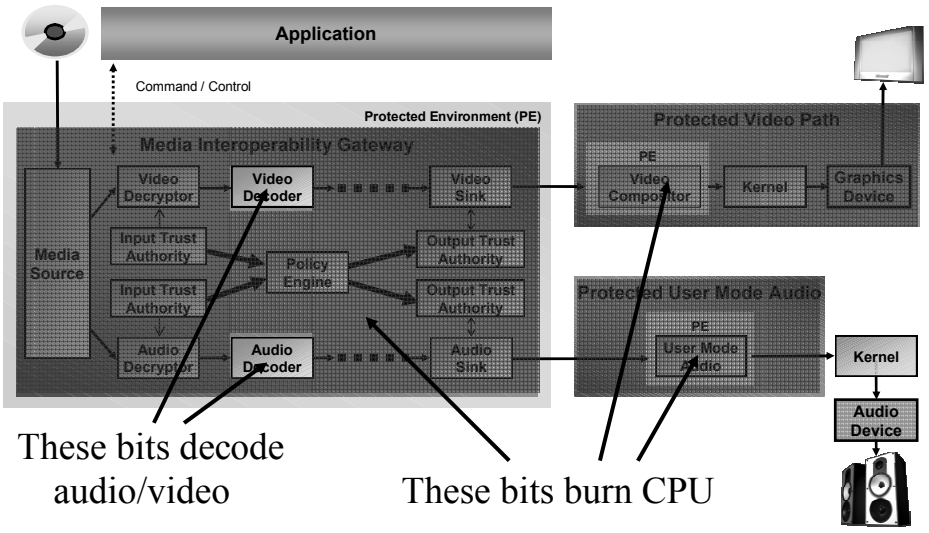
- A mass of assorted drivers has to wake up thirty times a second just to ensure that… nothing happens

Further device-specific polling also takes place

- Vista checks tilt bits on each frame of video displayed

This may explain the multiple reports of video and/or audio playback stuttering

# Additional CPU Consumption (ctd)



## Additional CPU Consumption (ctd)

Pages containing graphics content may be paged to disk

> Pages in the graphics subsystem can be paged out by the operating system when the need arises

- Wouldn't normally happen, but an attacker could induce paging deliberately
- Precious content could be paged to disk!

Vista tags pages containing content to indicate that they need to be encrypted by the pager

- Nothing else (crypto keys, banking PINs, personal data, medical information, …) gets this level of protection

A single frame of the FBI copyright warning is treated as being more valuable than a user's banking PIN

## Additional CPU Consumption (ctd)

Insufficient CPU power available to perform all of decompression, rendering, and video stream en/decryption

- At the time the content-protection spec was written, the fasted available P4 EE wasn't up to the task

  Since [encryption] uses CPU cycles, an OEM may have to bump the speed grade on the CPU to maintain equivalent multimedia performance. This cost is passed on to purchasers of multimedia PCs

  — ATI

## Additional CPU Consumption (ctd)

So we'll just wait for faster CPUs to appear…

> One developer said he couldn't reproduce the problem on his quad-CPU 4GB RAM machine with 4 striped RAID array disks
> — Con Kolivas interview (speaking about Linux developers' attitudes to performance issues reported by users)

Standard geek fallacy, "everyone's running a machine as fast as my desktop Cray, what's the problem?"

## Additional CPU Consumption (ctd)

Dell, HP, Gateway, … PCs come preloaded with a mountain of cycle-stealing crapware

Many PCs are so infested with malware that they can barely perform their normal tasks

- Depending on whose surveys you believe, the typical PC contains 20-30 pieces of malware
- Bill Gates (and others) have estimated that > 50% of all PCs are "no longer under the control of their owners"

## Additional CPU Consumption (ctd)

Even before factoring in the additional overhead of crapplets and malware, systems may be struggling to cope

> VAIO computers may not support movie playback on packaged media recorded in AVC or VC1 formats at high bit rates
>
> — Sony disclaimer

CPUs are never fast enough

- (Reviewers tend to use the latest hardware and a fresh OS install so they often don't notice these problems)

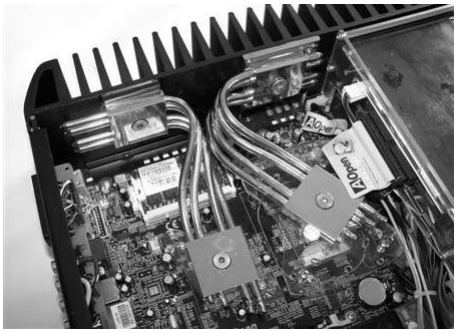
## Additional CPU Consumption (ctd)

Little acknowledgement of CPU budget issues, no acknowledgement at all of power or thermal budgets

- Not just "everyone has a desktop Cray", but everyone's running off limitless mains power

Also affects passively-cooled HTPCs, which have mains power but tightly constrained thermal budgets

- (Very difficult to get HW vendors to go on record about this)



## Additional CPU Consumption (ctd)

Laptop components are prevented from entering power-saving mode by unnecessary content-protection overhead

- Ripped DivX on an SD card: Only the LCD and GPU doing the rendering are powered
  - CPU, DVD drive, hard drive, … are suspended
- Protected content: DVD drive, CPU, GPU, and LCD (i.e. all major system components) are under load
  - Same problems were found with MP3 players and protected content, 25% higher power consumption across a range of products

Coming soon to Slashdot: "Windows Vista causes global warming!"

## Additional CPU Consumption (ctd)

Hardware must have video rendering support to compensate for the CPU overhead of content protection

- Requirements specify IDCT, MPEG motion compensation, and Windows Media VC-1 support in hardware

  It is a PVP-UAB requirement that discrete graphics chips implement at least iDCT and Motion Comp decode acceleration for MPEG2 and Windows Media® Version 9/VC-1
  - Like MPEG, VC-1 is also DCT-based so IDCT supports both MPEG and VC-1

## Hardware Resource Consumption

Devices are required to implement (at least) AES-128 in hardware

> Compliance rules require [content] to be encrypted. This requires additional encryption/decryption logic thus adding to VPU costs. This cost is passed on to all consumers
> — ATI

GPUs can do this by throwing out a few rendering pipelines/stream processors

- The low-end nVidia G84 and ATI HD 2400/2600 GPUs actually do this
- In high-end GPUs, the graphics performance takes precedence over content protection

## Hardware Resource Consumption (ctd)

Graphics vendors are in a bind

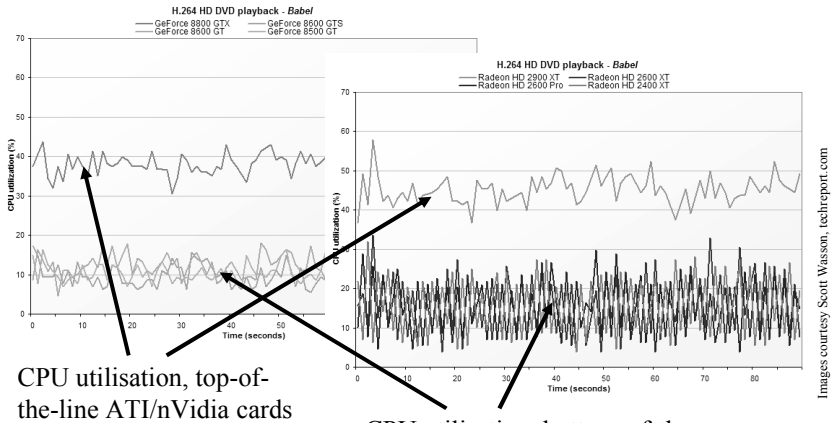
- Can't afford to give up die space and drop performance at the high end in order to accommodate content protection and HD playback
- If only one side makes the sacrifice, the other wins

It's a zero-sum game, neither side can afford to give an inch at the top end

- (Unless either all sides agree to make the sacrifice or one side is so far ahead that they can sacrifice the die resources)

# Hardware Resource Consumption (ctd)

Result: A $100 bargain-basement card outperforms a $1000 top-of-the-line card for HD content playback




Images courtesy Scott Wasson, techreport.com

CPU utilisation, top-of-the-line ATI/nVidia cards

CPU utilisation, bottom-of-the-line ATI/nVidia cards

# Content Protection Redux

If in doubt, disable it

- Many problems reported in playing back legitimate HD content under Vista

  I've just had my first experience with HD content being blocked. I purchased an HP Media Center PC with a built-in HD DVD player, together with a 24″ 'high definition' 1920 × 1200 HP flat panel display (HP LP2465). They even included an HD movie, 'The Bourne Supremacy'. Sure enough, the movie won't play because while the video card supports HDCP content protection, the monitor doesn't.

  It plays if I connect an old 14″ VGA CRT using a DVI-to-VGA connector

  — Roger Strong

## Content Protection Redux (ctd)

When I disable my HD monitor, I can watch the movie, on my old VGA screen, but, what is the point of having a HD monitor and not being able to watch a HD movie on it

— "muslix64"

I build 2 Media Center 2005's one for Satalite and one for Cable TV. Never had a problem recording my kid's show's. Upgraded to Vista MCE/Ultamite and like most people not able to record there 'Standard definition' HBO. So abviously the technology existed but now with Vista's DRM it is now being envorced much more strictly then the previous operating system's Microsoft has made

— "Lupo"

## Content Protection Redux (ctd)

The funny thing is that I can't see how HDCP will actually even prevent piracy. In fact the only thing I can see it doing is encouraging piracy because everyone whose bought a new computer/monitor/HDTV in the last few years which don't have HDCP are now screwed out of the several thousand dollar purchases. So instead of buying new products they will turn to pirated/cracked Blu-ray/HD-DVDs which will work without the HDCP

— "Gizza"

Analysis

## Analysis

The first listed Vista graphics requirement isn't the ability to handle Vista's much-touted new graphical interface (Aero et al)

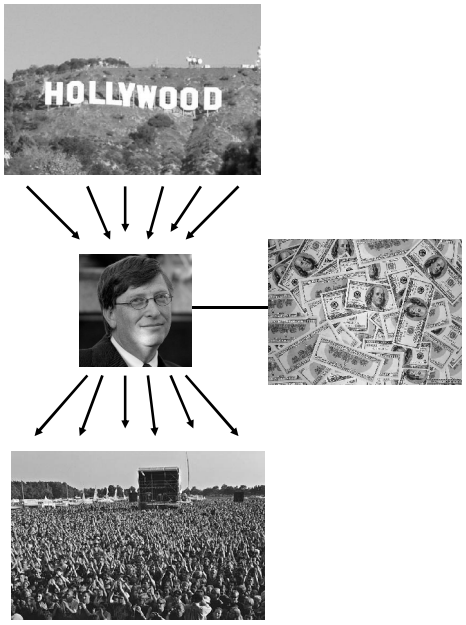
GRAPHICS-0001: Display adapter supports output connectors with content protection features and provides control via PVP and COPP DDIs

- The user interface comes at position 2

GRAPHICS-0002: Display subsystem meets GPU, memory, resolution, and bandwidth requirements for a premium Windows experience

This list seems to place content protection before all other graphics requirements for Vista

# This is not Rocket Science




# Possible Microsoft Thinking

Consumers are locked in

Competitors are locked out

> How do I put all these companies in a position where, regardless of what they see is in their best interest, they have to adopt your technology?
>
> I realized that a major part of my job was to figure out how to use technology control to create economic force, or leverage, such that money and business flowed in Microsoft's direction
>
> — Alex St.John, father of DirectX

## Possible Microsoft Thinking (ctd)

Frog boiling 101

- Currently (relatively) few Vista systems deployed, little premium content available
  - Consumers have little choice but to buy Vista, but they don't notice much
- Vista starts to become more widespread
  - Out-of-support XP is such a malware target that it's no longer usable
- More premium content appears
  - Even this term is misleading: In a few years everything will be "premium"
  - Content is "commercial content generally, independent of resolution" (Microsoft)

## Possible Microsoft Thinking (ctd)

Frog boiling 101 (ctd)

- Eventually everything is "premium" → everything is protected
- By then it's too late…

At this point Microsoft controls the distribution channel

- Like Apple, they can dictate terms back to content producers
- Play by our rules or we'll shut down your distribution channel

## Everyone Else's Thinking

> [The restrictions] will serve to make the illegal product the most full featured and least restrictive, and thus the most attractive to the consumer. Add in the expense of buying new equipment to view the legal content (when existing equipment is perfectly capable) and the performance drain imposed by in-line encryption/decryption and they've put out the biggest incentive to piracy yet
>
> — "Greg"

> Digital rights management technology will still fail to prevent widespread infringement. In a related development, pigs will still fail to fly. I predict that every year, and it turns out to be true every year
>
> — Ed Felten

## Everyone Else's Thinking (ctd)

> I could not be more skeptical about the viability of the DRM included with Vista, from either a technical or a business standpoint. It's so consumer-unfriendly that I think it's bound to fail — and when it fails, it will sink whatever new formats content owners are trying to impose
>
> — Matt Rosoff, lead analyst, Directions On Microsoft

- (HDCP is already strangling HDMI)

> The beatings will continue until market penetration improves
>
> — "NBarnes", slashdot

## Monoculture Meets Polyculture

Content-protection design docs seem to assume a hardware monoculture built from lots of readily interchangeable black boxes

- Any non-protected component can be trivially replaced by a protected component that fits into the same-shaped hole

In reality however the PC market is fantastically diverse

- The Barnum effect, "we've got something for everyone"

## Monoculture Meets Polyculture (ctd)

An interesting PC ecosystem adjustment will happen

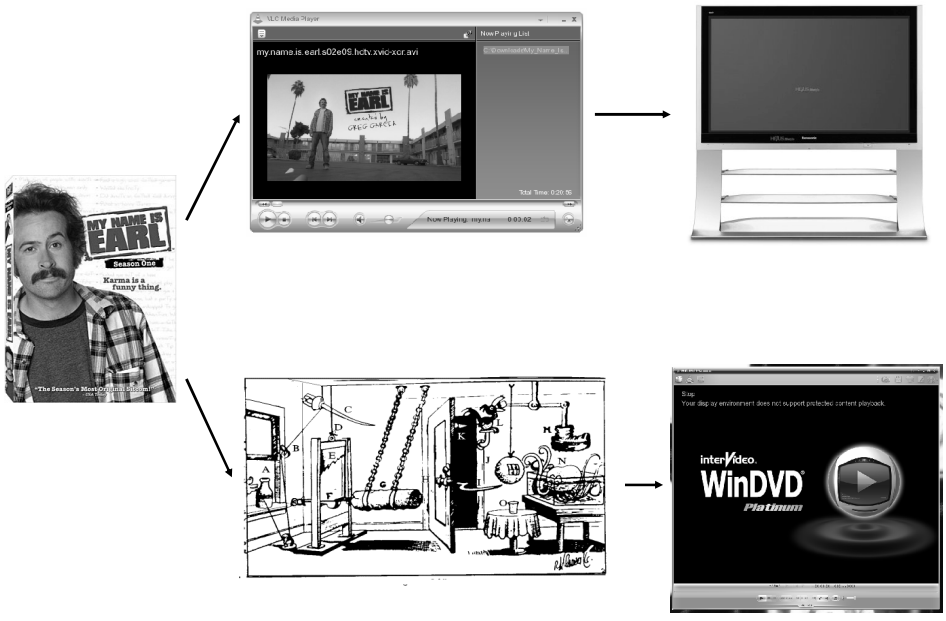
It just doesn't work this way

- You can't decide to change people's hardware because it's convenient for you, it has to be convenient for them
- (In addition users aren't going to give up their gainclones and Blowtorch preamps and Tice clocks in a hurry)

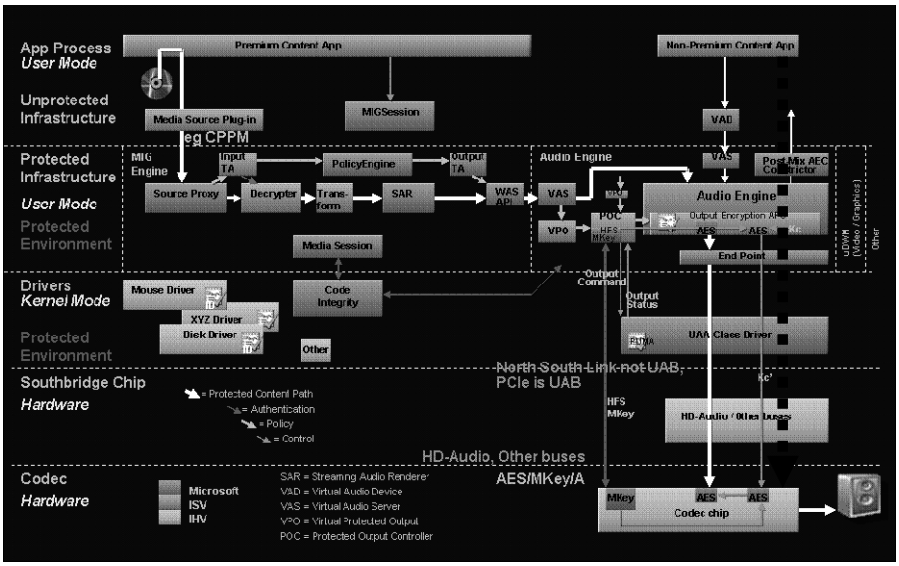
These assumptions were based on nothing more than wishful thinking, or on the fact that it would be very convenient if certain things were true

— Threat model analysis of the Walker spy ring, Laura Heath

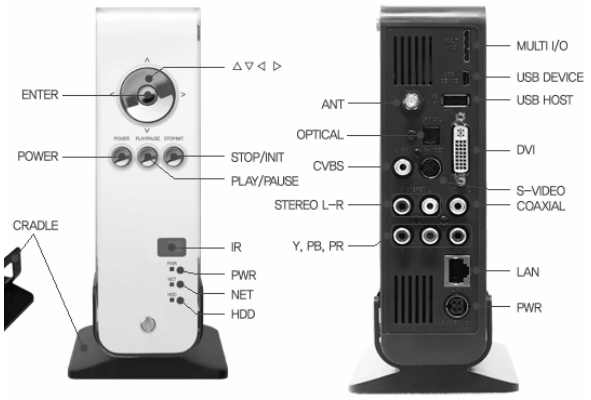
# It's Still not Rocket Science




# The Geek version, in Microsoft's own Words



# A bit of Perspective: The Competition




- About the size of a hardback book, silent, low-powered, sits on a shelf next to your TV, costs $80-100 (without HDD)
- Plays MPEG-1, MPEG-2, MPEG-4, DivX, AVI, WMV, AVI, MP3, Ogg Vorbis, WMA, …

# Oh the Humanity!

Consider what all of this wasted effort could have been put towards…

- Encrypted paging → protect user secrets
- Protected content domains → keep out malware
- Anti-debugging techniques → prevent rootkit hooking
- Protected output path → trusted I/O for user credentials

… and on and on

## Oh the Humanity! (ctd)

Imagine if all of this wasted effort had been put towards protecting Vista's users instead!

> We want to make the PC a safer place for premium audio content, in the same way that we're making it safer for premium video content

What about making it a safer place for the user?

## There is No Escape

Hardware vendors have to drink the Cool-Aid

> There is no requirement to sign the [content-protection] license; but without a certificate, no premium content will be passed to the driver

- Since Windows is the primary market for PC hardware, every vendor will have to build this stuff into their products

Whether you use Windows Vista, Windows XP, Windows 95, Linux, FreeBSD, OS X, Solaris (on x86), or anything else, Vista's requirements will make your hardware more expensive, less reliable, more difficult to program, and more difficult to support

- This affects *everyone*, not just Vista users

Why did they Do It?

## Why did they Do It?

The original intent wasn't to protect HD-DVD or BluRay or Internet content at all

- They didn't even exist at the time

The target was standard over-the-air/cable analog TV

- Yes, you can copy that using a VCR, the MS techies knew that too
- Ours not to reason why…

## Why did they Do It? (ctd)

For the MS marketers, HBO, PPV movies, … were the holy grail

- This lead to more and more lawyer-driven requirements being added

The main technical problem to overcome was the inability of the PC to control set-top boxes

- No closed-loop control system for set-top boxes existed
  - You could spoof a remote via IrDA and screen-scrape the results, but… ugh
- No incentive for vendors to standardise any external control API

## Why did they Do It? (ctd)

Solution: Move the set-top box into the PC

- Hey, our set-top box now has a fully-featured OS, an Internet connection, a …
- HP can make a nice profit replacing a $50 Chinese-made player with a $1000 Media-Center PC

Fears of Tivo-style lawsuits (30-second ad skip) paralysed the Media Center group

- You can't remove commercials in content that you don't control and can't copy

## Why did they Do It? (ctd)

In the meantime, the developers couldn't even get the code to work properly for plain non-premium content

In mid-2007, Microsoft finally rolled out digital cable-enabled PCs

- A complex mess: 1996 Telecommunications Act mandated open access, the FCC sort-of giveth, CableLabs taketh away again
- Microsoft and ATI created the Open Cable Undirectional Receiver (OCUR) specification for in-PC cable boxes

## Why did they Do It? (ctd)

Need to be a Microsoft-approved OEM partner to sell PCs with OCUR cards

- Can only be obtained as a complete unit: PC + OCUR + Windows Vista
- Currently almost unobtainable, cost several thousand dollars

If this is an indication of Microsoft's premium content delivery system, we're in trouble

> I haven't witnessed a product rollout botched this badly since Microsoft introduced the Zune
>
> — "PC + Digital Cable = Not Ready for Prime Time", Michael Brown, MaximumPC editor

## Why did they Do It? (ctd)

OCUR systems took 18 months to appear after the spec was finalised

- They didn't… really… work very well

  Click the Start menu and then click on Computer. Now, point the mouse to Local Disk C, but hold the shift key down when you left-click with the mouse. When the menu pops up, click on Open Command Window here. Now, type this command in, but you have to type it in exactly right or it won't work. Type c colon, backslash, ehome, backslash, ehribjob.exe forward slash all caps OCURN lower-case register

  — Microsoft tech support
- http://www.maximumpc.com/article/ocur makes for amusing/scary reading

## Why it's such a Mess

Content protection is the Vietnam/War on Drugs/*insert analogy here* of Microsoft development

A death march, but worse

- On a standard death march, at least the customer wants what you're working on

## Life Cycle of a Content-protection Developer

New developers turn up bright-eyed and bushy-tailed

- "Wow, this is an amazing technical challenge"
  - The Reindeer Effect, hack away at something because it's a challenge
- (Even if they don't necessarily believe in what they're working on)

Start coming up with ideas for solutions to various problems

- Begin work on implementing some of them

## Life Cycle of a Content-prot.Developer (ctd)

Discover more problems

- Example: AEC issues
- Back to the drawing board
- More possible solutions, more code to write

More problems…

- Example: What constitutes a UAB?

# Life Cycle of a Content-prot.Developer (ctd)

Eventually they burn out and leave

- Transfer elsewhere within MS
- Leave the company altogether

The next wave of victim^H^H^H^H^Hdevelopers moves in, picks up the more obvious pieces, and the cycle starts anew

- The only thing missing is the “Abandon all Hope ye who Enter Here” sign over the door

# Questions?

## (Footnote slide)

Some Microsoft folks who provided feedback on the slides pointed out that a few of the issues here are somewhat contentious, with several (like the DRM debate) being perpetual-motion debate topics that are just too complex to cover here. The following links provide starting points for further reading

- "We need new protection mechanisms in order to explore new business models for content" is the argument used for passing the DMCA. Both pro and contra points of view have been extensively documented, a starting point is http://en.wikipedia.org/wiki/Dmca
- Larry Osterman's blog has a good discussion of DRM from both points of view. You can read the entry at http://blogs.msdn.com/larryosterman/archive/2005/04/28/413055.aspx

## (Footnote slide ctd)

*…continued…*

- What happened with the USS Yorktown was covered in some depth in the RISKS forum, starting at Volume 19, Issue 88, http://catless.ncl.ac.uk/Risks/19.88.html. It continues over further issues of RISKS, with comments from various sides of the debate
- The debate over driver signing, what it's intended to achieve, and the Atsiv revocation, is covered from both sides in the MSDN Vista Security Blog at http://blogs.msdn.com/windowsvistasecurity/archive/2007/08/03/x64-driver-signing-update.aspx

## (Footnote slide ctd)

*…continued…*

- Verisign doesn't have an acceptable use policy (AUP) for code signing specifically, but it does have a general certificate practice statement (CPS). The revocation reasons listed are (of necessity) vague enough to cover revoking almost anything, you can find them at http://www.verisign.com/repository/CPS/VeriSignCPSv3.5.pdf
- Verisign's web page for reporting misuse of code signing is at http://www.verisign.com/support/code-signing-support/code-signing-misuse/index.html although none of the example misuse types listed cover Atsiv

## (Footnote slide ctd)

*…continued…*

- The list of Windows Vista graphics requirements (which may or may not be priority-ordered :-) is at http://www.microsoft.com/whdc/winlogo/hwrequirements.mspx
- The misuse of surveillance systems in ways not intended by their designers was covered in IEEE Spectrum, http://www.spectrum.ieee.org/print/5280