Peter Gutmann on Vista DRM

Description: Peter Gutmann, the author of the highly controversial white paper detailing the significant cost of Windows Vista's deeply-entrenched digital rights management (DRM) technology, joins Leo and Steve this week to discuss his paper and his findings.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-074.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-074-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

Leo Laporte: Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 74 for January 11, 2007: Peter Gutmann and the cost of Vista content protection.

Security Now! is brought to you by Astaro, makers of the Astaro Security Gateway, on the web at www.astaro.com.

It's time for Security Now! with the fabulous Steve Gibson. And this in some ways is a part two. Last week we were talking about some pretty tough stuff: content protection, the new AACS content protection that's going to be part of Vista, part of any HiDef DVD player you have. All of this was kind of prompted by an article that just spread like wildfire over the Christmas break.

Steve Gibson: Right, well, it generated a lot of controversy because it became clear from the article published by Peter Gutmann, who's in New Zealand, a New Zealand-based, very well known, good reputation security analyst. He took a look at the consequences of essentially putting this AACS, the Advanced Access Content System, which has been assembled by a number of hardware companies in order basically to appease the interests of Hollywood, in order to say, look, this is the way we're going to protect the next generation of content.

As we saw last week – and the reason we spent last week's episode was to create some historical context for both the legislative side and the technical side. And I talked last week about basically AACS is a phenomenally complex technology that involves state-of-the-art encryption. It involved some stuff you just can't even get your mind around. I mean, I will never try on Security Now! explaining the subset difference tree system for allowing keys to be revoked by keeping those specific players from being able to perform the decryption. It's mind-numbing, what they've done.

And so it's one thing for that to be in an HD-DVD player. And in fact we've already seen, consumers have seen the consequence of that when they stuck a DVD into their first-generation players, it would take up to or in some cases more than a minute for the player and the disk to negotiate all of the crypto going on just internally within the player. And Leo, I was thinking about how you had commented that, when you stuck your HD-DVD on your Xbox 360, it didn't take long.

Leo: Well, it's got a faster processor.

Steve: Exactly. Well, talk faster, that's a monster.

Leo: It's got three 3GHz Power PCs...

Steve: Exactly. Exactly. So it's a very different platform there than a typical consumer drive, where they're trying to keep the cost as low as possible.

So anyway, I'm excited. We're going to have Peter joining us here in a moment from New Zealand because we wanted to talk to him, get his side of this, talk about what the paper that he wrote is about. And I just wanted to sort of give a little bit of a preface and explain that basically Microsoft has decided that they want Vista to be able to deliver this kind of content. And what Peter's paper is about is essentially the cost of delivering this content. And what it means is that so many aspects of our PCs, which have been fully documented, been public domain, been anyone could develop a display card, for example, that's no longer the case. If you're going to have any foot in this next-generation game, you have to sign up and apparently pay hefty license fees just to participate. And if you don't get certificates, which are subject to spontaneous revocation, if you then subsequently misbehave, or in fact I read one of the AACS organization documents said that you could be revoked if you failed to pay your annual dues.

Leo: Your card would stop working in my PC.

Steve: Exactly. The hardware that the consumer purchased could be shut down.

Leo: Never buy a card from somebody who's about to go bankrupt.

Steve: That's a very good point.

Leo: I mean, the whole thing is nuts. This is just nuts. We're going to talk to Peter in just a bit and get the details. But I want to thank, before we get going here, I want to thank Astaro Corporation, our sponsor for Security Now!. They really support us financially, and they make this show possible. And so you could do us a favor. If you're a small or medium business looking for some real protection, not just anti-hacker or firewall, we're talking spam, viruses, VPN and intrusion protection, content filtering, too, this is an industrial-strength firewall. It's a complete protective device. It's a simple, easy-to-use appliance. And you can try it for free. Just call Astaro, Astaro.com, 877-4AS-TARO, and they will set up a free trial of an Astaro Security Gateway in your business. We've talked to many, many people who have done this and are very happy that they heard about Astaro on Security Now!. And by the way, if you're a non-business user you can also download the software for free: www.astaro.com. We thank them for their support.

Let's call New Zealand, what do you say?

Steve: Let's talk to Peter. Great.

Leo: Let's just start off the interview by asking you about your background. You're a fairly well-known security researcher, I gather a computer scientist, as well.

PETER GUTMANN: So my background is – it's actually a bit of both academia and industry. I have an open source security toolkit which is available under a dual license, so it's both GPL or commercial. It's a Sleepycat license, if you're familiar with that. And people can choose what they want. And when I'm not working on that, I get to play with any kind of security stuff that happens to interest me. So, for example, with Vista, just before Christmas I had a bit of spare time. And some people had been talking about this in private, and I started going out and looking at the specs and was kind of frightened at what was in there. And so I thought I should maybe do a write-up of this, an analysis, to let people know exactly what's hiding inside Vista.

Steve: In fact, it was because of Peter's crypto toolkit that he and I first had a dialogue. It's funny, when I was sending email back and forth to him it was disappearing into one of my folders, and it took me back to a conversation Peter and I had had briefly back in 2002, about five years ago, and I was asking him about the licensing terms for his toolkit because I was looking around for something that I could trust to sort of use for core crypto stuff. And so we had a dialogue back and forth. And of course Peter's also done some work in secure hard drive erasure. And he has an often-quoted piece of work that talks about how to deeply erase magnetic media. And so of course from my background with SpinRite there was another connection there. So I've seen Peter's name around a lot.

And in my case someone, I think it was in the GRC newsgroups, posted a link to Peter's article. And as I mentioned on our podcast last week, I printed it out, didn't have a chance to read it before taking off to travel for the holidays. But I was on an airplane flying home, and by the time I was on the second page I was just riveted by the content. And of course, as we talked about last week, essentially there's a next-generation crypto system for protecting high-value content, which is known as AACS. And what Microsoft has done is they've decided they're going to make Vista be a valid, secure delivery platform for AACS-protected content. And so basically what Peter's paper does so well is to open people's eyes about the real-world consequences of turning Vista into a sort of a next-generation DRM platform.

Leo: For those of you who haven't read it, it's called "A Cost Analysis of Windows Vista Content Protection." Let me just give you the executive summary, and then we can go point-by-point through some of these things.

Steve: Or the executive executive summary.

Leo: I know, I love the short-short version. But let's start with the little longer version. Windows Vista includes an extensive reworking of core OS elements in order to provide content protection. That's that AACS you're talking about for premium content, typically HD data from Blu-ray and HD-DVD sources. But here's the gist of it. Providing this protection incurs considerable costs in terms of system performance, system stability, technical support overhead, and hardware and software costs. And these issues affect not only users of Vista, but the entire PC industry, since the effects of the protection measures extend to

cover all hardware and software that will ever come into contact with Vista, even if it's not used directly with Vista, for example hardware on a Macintosh or on a Linux server. Then the executive-executive summary: The Vista content specification could very well constitute the longest suicide note in history. You read all of that stuff, Peter?

PETER: Yeah.

Leo: There's a lot of material online from Microsoft. I mean, they're not keeping this a secret.

PETER: No. Well, the best paper is the first one I give in the references, the "Output Content Protection and Windows Vista," which was presented at the WinHEC conference in 2005 by Dave Marsh, who is the program manager for, as far as I can tell, for DRM inside Microsoft. And that goes into an extraordinary level of detail about all this stuff. But, yeah, they have a number of other public papers that describe what they're trying to do.

Steve: One question I had, and I've read the AACS specs, and I've got sort of, I think, a relatively good handle on what AACS is, I didn't see in the specs anything about this notion of constriction. And I'm wondering if that's something that Microsoft has done to sort of try to appease the content owners while not completely disabling non-securable outputs.

PETER: Right, well, the thing is they're terrified about the analog hole. Well, not so much Microsoft. I think Hollywood is terrified of the analog hole. And so they're desperately trying to make sure that, you know, they can't close it entirely, but they can at least make the quality of the content that goes through the analog hole so poor that it's not worth copying.

Steve: Right. Do you have some sense from – I know that you mention in your paper that you have other sources that have required that they remain anonymous, and in fact you went to the length of deliberately restating some of the things they told you, trying to maintain accuracy, but really to protect their identity.

PETER: Right.

Steve: And so the one thing I'm wondering is, can you give us some sense for where this is coming from? That is, how much of it is push from Hollywood and how much of it is Microsoft sort of trying to deliver something maybe that no one really wants?

PETER: I think it's a bit of both. I mean, Hollywood has this huge wish list of stuff that they've been pushing for years and years. And, you know, people have analyzed the technical side of things and see that what they're trying to do is impossible, you know, in terms of closing the analog hole and making content uncopyable. There's a wonderful quote from Bruce Schneier saying that trying to make content uncopyable is like trying to make water not wet.

Leo: I love that.

PETER: And there's a whole lot of legal CYA in there in the specifications where they say device manufacturers must demonstrate their commitment to the party line. Rather than saying you must do this, this, and this, they say you must demonstrate that you're strongly committed towards content protection. And I think probably what Microsoft is doing is the same thing. They want to demonstrate to Hollywood that they're really, really committed towards content protection.

Leo: That's a lousy specification, not telling you what to do, but just saying prove it.

PETER: Right. But...

Leo: Prove you care.

PETER: Yeah. But the problem is a lot of this, I think, is driven by legal worries. And so if they say you must do this, and then it gets broken, they're in trouble.

Leo: Ah. So they can't be specific.

PETER: Right, they can't afford to be specific because, if they end up being wrong, then they're liable.

Steve: And I guess one of the things that is not immediately obvious, even in – well, I guess your paper sort of began me thinking down this direction. But then reading the AACS stuff and looking at the revocation technology which has been bundled into this, it's very clear that, while Microsoft is bearing some responsibility, there's a tremendous onus also put, for example, on graphics card makers. I mean, they're hugely incentivized to make their cards perform and their drivers perform really at a level of quality that we've never asked from them before.

PETER: Right. And that's particularly nasty for them because they're not given any hard and fast rules. They're just told that you'd better show a lot of compliance. And if it's not enough, you can guarantee that you'll be in hot water.

Leo: Well, Paul Thurrott, who does a Windows podcast for us, made the point – I'd like to hear you address it – that the alternative for Microsoft is to be a second-class citizen in terms of supporting content. You play by Hollywood's rules, or you don't play at all. What's your response to that?

PETER: I think that's very much a red herring. And in fact I've been updating the document constantly to cover this, and I addressed that in a very recent release. Microsoft owns, I don't know what it is, 95 percent of the market or so. And particularly for desktop OSes, they own pretty much the entire market. They could quite easily say to Hollywood, you know, we're not going to put this stuff into the operating system because it severely degrades the performance and reliability and stability and so on and so forth. Take it or leave it. You know, this is assuming that Hollywood relies entirely on Microsoft – sorry, that Microsoft relies entirely on Hollywood. Well, Hollywood relies entirely on Microsoft. If Microsoft said we refuse to do this, Hollywood can't afford to ignore 95 percent of the market. So I think that's a bit of a red herring.

Leo: So companies like Apple, people who make Linux distributions, could safely ignore this content protection and say, well, you know, we don't have to do it, let Microsoft do it, we won't do it.

PETER: Right. And that's, you know, so the example you cited of the suicide note, that was actually taken, just as sort of a bit of background information, that was taken from the British Labour Party's 1983 election manifesto, which someone said was the longest suicide

note in history. The Microsoft suicide note is a bit longer. But the thing is, that was so bad that their opponents actually printed it out and used it as propaganda for their own cause. And so it could well be that Apple's going to go and point out some of these really nasty things inside Vista and say, look at how bad this is. Buy our computers and our operating system instead. And certainly the Linux people are going to use it for propaganda to make Linux look good.

Leo: Right, right. So this is a technical podcast. So I think we should probably, Steve, walk through these various consequences of this copy protection scheme, especially since we've already talked about AACS in detail last episode.

Steve: Right. I think that the point that Peter's paper makes so well is that – and this is actually how he and I began corresponding via email – is that the PC has traditionally been an open platform. I remember very clearly when I got my very first real IBM PC with, ooh, a big 10MB hard drive, the technical reference manuals you could get with it had the schematics of the machine and the source code of the BIOS, just provided by IBM as part of the package. And that really sort of came from Apple because the Apple II had the same thing.

Leo: And it really kick-started the PC revolution.

Steve: Oh, I mean, my first PC application was a little thing called FlickerFree which replaced a chunk of the IBM PC BIOS because it was so poor at scrolling the CGA, the color graphics adapter card. And so I was hugely empowered by the fact that IBM had left the platform so open. And of course everyone remembers how the PC just exploded with all this add-on software and hardware. And of course IBM famously sort of backed away from their open stance when they created that horrible Micro Channel Architecture, which was pretty much stillborn. But still, I mean, ever since then the PC has been fully documented. You could get specs. You could find sample code. I mean, it's just been this tremendous environment. And what really upsets me is to do what Microsoft has decided they're going to do requires closing down major chunks of the architecture.

Leo: Well, let's start with Section 1, disabling of functionality. And you talk about how S/PDIF will no longer work with protected content. You talk about how, if you bought a video card that supported HDMI digital video with HDCP, you're going to have to buy another one because they didn't really work when they first came out?

PETER: Right. So the problem with that is, in order to – HDMI is basically a slight variation of the standard DVI output that you have on things like LCD flat panels. In order to protect that, you have an encryption mechanism called HDCP. And to do that you need to put encryption keys onto your video card. The problem is that it costs money to put these individual encryption keys onto each video card. So to reduce costs, the card manufacturer has simply omitted them. So if you bought a supposedly HD-ready video card...

Leo: It won't work.

PETER: It won't work because it doesn't handle the encryption.

Leo: If you spend money on S/PDIF, it won't work because it has to be disabled because there is no protection on that.

PETER: There's no protection whatsoever, yeah. And that's the nasty thing with sort of audio fanatics or anybody who basically wants to produce high-quality audio from a PC or use some sort of digital interface and maybe even optical output, connected to some expensive amplifier or whatever. And because there's no protection involved in the audio output, that has to be disabled.

Leo: Now, we should make that clear. It's disabled only when you're playing back protected content like an HD-DVD or a Blu-ray DVD. I mean, it's not always disabled.

PETER: It's not always disabled, no. On the other hand, it's problematic because, if you look at the Windows specs, sorry, the Microsoft specs for the content protection, let's say you're playing – you're making a Skype phone call and in the background you're playing some protected-content music of some kind. Because that all goes through the same sound output system, that kind of infects everything. So the protected content infects every other content that happens to be going through the system at the time.

Leo: We in fact wouldn't be doing this interview now because I use optical outputs. So they'd be shut down.

PETER: Well, they're not exclusively shut down. Again, reading the specs, I think probably what most manufacturers would do is just shut it down. But what the specs say is that, depending on how much protected content is present, you partially shut it down. So, for example, if you're playing protected content, and it's very quiet, then some of it will be shut down; and as the volume increases, more of it gets shut down.

Leo: There's also this issue – and this is to prevent the analog hole, I gather – of disabling or really reducing quality of other outputs so that, if you don't have HDCP, you can watch it, but it's really only 480i.

PETER: Right. So Microsoft say that any display device that has a resolution of more than 520K pixels, which in practice is a resolution of about 800x600, has to have its output degraded. Now, if you look at the Vista specs, in order to run Aero you need a resolution of 1024x768. So basically it means that anything connected to a Vista machine running the Aero interface will have its output degraded.

Leo: When will the output be degraded?

PETER: If there's premium content present.

Leo: Unless you have an HDCP-enabled card?

PETER: You need an HDCP-enabled card and an HDCP-enabled display.

Leo: Ah, so my display isn't going to work.

PETER: Right. So it's, well, even then – so what Microsoft just did is you have to put a piece of hardware into your video card called a "constrictor," which basically downscales the video to some extremely low resolution and then upscales it back again. So effectively you get a very low-quality output. But because this requires custom hardware or custom drivers or whatever, stuff that the manufacturers haven't actually been able to put into their cards yet, it seems that at the moment when people are trying to play HD content or premium content, they simply don't get any output at all.

Leo: Great.

Steve: So it was my feeling, and I guess this is from something I read in some forums, that in fact the current HD-DVDs would play, for example, on a consumer HD-DVD player, even out of their component outs, because the policy that goes along with the content was not yet so restrictive that the policymakers were saying we're not going to allow analog output to happen.

PETER: Right, yeah, because they're so afraid of consumer rejection. I mean, obviously, if you've bought an HD player and some huge plasma screen and spent thousands of dollars, and you put a disk in, it doesn't play, you're not going to be very happy. So at the moment, yeah, they're turning off this constriction. However, how Windows handles this is another matter. If you look at – I've been reading a pile of web forums about this. And the thing you see over and over again is I bought a computer, it came with an HD drive, I put the disk in, it didn't play. So maybe Windows doesn't honor that or doesn't handle it that well.

Leo: It's interesting because I have an Xbox 360, also from Microsoft, with an HD-DVD drive. It doesn't have HDMI out, doesn't obviously have HDCP. It plays high-quality over component outputs and looks great. I guess they just haven't enabled it. I mean, here's a Microsoft product where they haven't made that compromise.

PETER: Right.

Leo: You think that Vista will.

PETER: From the reports from beta testers and so on, from the reports we've been seeing, I mean, it's really hard to predict the future because it hasn't been officially released yet. But from reports from beta testers, a standard complaint is that they put the disk in the drive and it doesn't play.

Leo: Let's talk about some other consequences of this copy protection. Some of these are serious to a limited audience. For instance, open source hardware support, it's now going to be very difficult to write an open source driver for any of this hardware.

PETER: Right, yeah. So one of the things they require, one of the things they're worried about is someone creating some emulation of a hardware device, so you emulate perhaps some software, or perhaps some hardware, a sound card or a video card or whatnot. And then Vista sends the decrypted content to your artificial sound card, your artificial video card, and your thing got direct access to it. The reason why they're worried about that is

because this is exactly what people have done in the past under Windows XP. They've created sort of loopback devices or whatnot, and Windows has sent the content to some loopback device or some artificially created device driver that pretends to be the real thing.

Leo: This way you could capture keys and things like that.

PETER: Well, not so much capture keys, capture content.

Leo: The content itself.

PETER: Right. And so to disable this they require something called HFS, Hardware Functionality Scan. Which means that the device driver has to probe the hardware and try to determine whether it's genuine hardware or not. So it executes undocumented features or exercises some sort of undocumented functionality or pokes around inside the thing in such a way that hopefully it can't be faked by a malicious piece of hardware. The problem is, in order to do this you can no longer document the internals of the device because, if you did, then someone else could write an emulator for the device that pretends to be the real thing.

Leo: So you can't publish specs, and you can't publish source code.

PETER: Right. Now, again, the language in the spec is kind of wishy-washy. It doesn't say you can't publish any specs at all. It simply says that some aspects of the device will have to be kept proprietary. But that's kind of nasty for anyone writing open source software because, if you've got a graphics card, you need to know exactly how it works in order to write the drivers for it. And if half the thing is undocumented, it becomes very hard to support it properly.

Leo: Isn't it possible that just the undocumented part will be the premium content playback, and everything else will be documented; and you could still write a driver for Linux, for instance, but it just wouldn't play back HiDef movies?

PETER: Well, it's not that you can partition a card into one specific premium content, but everything else is public. What they are requiring that you do is that you exercise, and again the specs are vague, but some sort of functionality of the card, the graphics rendering engine as an example, like in several cases, and to determine whether it really is a genuine card or a copy of the thing or an emulator that someone's created. And leaving the whole graphics rendering engine undocumented is a pretty nasty denial of service on anyone who wants to write open source drivers for it.

Steve: Well, and the other thing that I think is really interesting, and Microsoft's spec makes this very clear, is they have this notion of a user-accessible bus. And essentially, if you have a separate graphics card – and they make a big deal about the difference between an integrated graphics subsystem on the motherboard, where you don't have a bus exposed, and this notion of a separate graphics card. Because again, that bus is an opportunity for someone to snoop the bus and capture content as it's going from the motherboard up to the graphics card. So there's a whole 'nother level of technology where essentially they're doing a modified AES 128 encryption on the fly at high bandwidth, which turns out to be very difficult to do.

PETER: Right. And I think the threat model for that is, if you've read the book "Hacking the Xbox," the guy who first sort of broke the security on the original Xbox...

Leo: Bunnie Huang, yeah.

PETER: Right, attached a FPGA-based logic analyzer to the system bus. And so they're trying to encrypt the system buses to stop exactly that sort of attack. It's kind of interesting, if you read through the specs and you think back, okay, what are they trying to defend against, here was a published attack, and presumably they're worried about exactly this kind of attack. And so they're taking these very unusual and probably excessive measures to try and defend against it. And the problem is, again from Microsoft's own documents, the current processes simply don't have the horsepower to do both video processing and encryption of high-bandwidth content.

Steve: The other thing that I found interesting was that Vista introduces this notion of a so-called "protected environment" where applications, or that is to say processes running within what Microsoft calls the "Vista protected environment," are inaccessible to a much greater degree than existing applications, for example in XP, would be, the idea being to prevent people from sort of the outside of this protected environment from being able to snoop into other things running on the same system.

PETER: Right. And that's one of the sad things about this whole Vista DRM effort. They've put a huge amount of work into creating this protected environment. Now, imagine if they'd instead used that to protect against viruses and malware and rootkits and so on and so forth.

Steve: Exactly. It's one of the things that I think I may have commented on last week was that, as you read this, you get a sense for this phenomenal amount of industry which has gone into turning Vista into this platform that can play HD-DVD and various types of other source forms of high-definition protected content. It's not something that it's clear that a majority of Vista users will even take advantage of. Yet even so, all that work was done instead of all these other features that we were supposed to be getting in Longhorn that were stripped out. And they've basically burdened the operating system with all this technology.

Leo: Well, ironically, they've made it more susceptible to malware. These tilt bits – talk a little bit about the tilt bits, Peter.

PETER: Right. So what tilt bits are is – the name's taken from pinball machines. We had tilt sensors to monitor physical interference with the device.

Leo: Yeah, if you pick up the machine and get the ball in the hole, it's tilted, and it fails.

PETER: Right. And so Microsoft have done or required that hardware manufacturers do pretty much exactly the same thing. The nasty thing with this is that, well, to put it bluntly, it makes your hardware in your system a lot less reliable. The typical PC is thrown together out of all sorts of random bits and pieces with different tolerances; and half the parts are made by the cheapest possible manufacturer, so a lot of them are cheap and nasty. So they're designed to have a certain amount of tolerance for voltage fluctuations and strange bus signals and bugs in device drivers that set hardware bits wrong and so on and so forth. The problem is that, if you do get these strange voltage fluctuations or strange noise on the system bus or whatever, that could also be a sign of attack. And so Microsoft have said that hardware has to monitor for any of these peculiarities. And if they're found, then it

sets these tilt bits in a register somewhere. Vista polls these tilt bits; and if any of them are set, it reacts in some vaguely specified but somewhat drastic manner.

Leo: Will it shut down, or crash, or put up a blue screen?

PETER: What the specs say is that – I'm just trying to find the exact quote because it's vague enough that I'm actually going to have to quote Microsoft rather than trying to figure out what it is they mean. Well, they say it initiates a complete reseat of the graphics system, and it also mentions it's a restart. Now, I don't think that's a restart of the PC as a whole. Presumably it's just a restart of the graphics subsystem.

Steve: Yes, and it requires a reauthentication of the whole system to be self-consistent internally.

PETER: Right. So I think the effect is going to be that, if any of these tilt bits get set, there will be some drastic amount of processing and change of system state going on in Vista. And I don't know exactly how noticeable it's going to be, whether it takes five seconds or 10 seconds or half a second or whatever. But whatever the case, if some slight glitch is detected, then Vista's going to do some serious reconfiguration of system state for some fixed amount of time before anything else can happen.

Leo: Which as you point out makes it just prime for a denial of service attack from malware.

PETER: Right. Well, yeah. I mean, if you want to cause a disturbance in the system, then just trigger one of the tilt bits and watch Vista drive itself nuts with doing a restart of the subsystem. But even then, you know, someone mentioned on a blog, and I think this is quite a neat quote, it was something like, "Tilt bits are quite clearly insane." And they are. I mean, what hardware manufacturer would voluntarily make their hardware less reliable and less stable? Which is what tilt bits are doing.

Leo: Does all of this content protection, okay, it affects reliability. Does it also slow the system down?

PETER: I would imagine it does because you've got this huge layer of bloat sitting in there, intercepting all audio and video output and content output and processing. This doesn't come for free. I mean, again, from the specs, Vista is certainly continuously polling and checking hardware and checking tilt bits and checking all sorts of other things.

Steve: Right. I was just going to say that the spec does require that software drivers at every 30 milliseconds, which is essentially 30 times per second, are going out and polling the hardware in order to maintain an intimate relationship with the hardware in order to try to catch anybody playing any games. So even when your system is not actively doing something, you've got drivers that are busy making sure that nothing continues to happen.

PETER: Right.

Leo: What you're describing is an operating system that is essentially insanely paranoid.

It's gone off the deep end.

PETER: That's true.

Leo: 30 times a second. Is it hacking me? I mean, that's crazy.

Steve: It really is. Now, there's one other aspect that has occurred to me since we last talked about this. I'd love to get Peter's opinion. People listening to this so far in our last podcast might be thinking, okay, so Vista's not going to let me watch HD, this newfangled content. But what has also occurred to me is that Vista is sort of retroactively going to become hostile to many of the things that people used to be able to do, for example, ripping DVDs, decrypting DVDs. Where the technology does exist for that, suddenly there's the ability to prevent that from happening, and that does seem to be what Vista is doing. So it's actually backing people away from things they were able to do historically under Windows 2000 and XP, taking things away.

PETER: Right. Although someone else has pointed out that the Vista content protection is so thoroughly obnoxious that it's actually going to be a major driver towards piracy.

Leo: You quote muslix64, the guy who came up with the crack of HD-DVD.

PETER: Right, exactly. I mean...

Leo: That was his incentive.

PETER: Yeah. The reason why he was doing this isn't because he's a pirate, but because he bought a system with all the HD components in, and he couldn't play back his video. So if you're an average guy, and you've gone out and bought a system with an HD player and high-resolution monitor and so on attached, you put in a disk and it won't play, what are you going to do? You're going to go out on the internet and find some software to crack the copy protection because it's preventing you from playing legitimately purchased content. So it could actually be a huge incentive towards piracy and towards bypassing the copy protection because it's so obnoxious that people just want to get it out of the way.

Steve: Peter, one other thing that I keep asking myself is we know, just due to the nature of physics, as you said in your white paper, it is impossible to do what Microsoft is trying to do, that is, there is no absolute control over the remote delivery platform. So it's going to end up one way or another being cracked.

PETER: Right.

Steve: And the people who have the most incentive are more the commercial-grade pirates that are really mass-producing pirated content. We know they're going to come up with a way around this. So to me this seems like a huge amount of burden to put on people's grandmothers who are never going to pirate this content. And they're doing it even though it can't be effective.

PETER: Right. Well, again, you've got the fact that you have to show a certain level of commitment to the cause. They can now go back to Hollywood and say we've done the best we

can towards showing that we're on your side. Give us the premium content.

Steve: So it's really not about who are they trying to target, it's saying to Hollywood no one to the best of our ability is going to be able to use PCs as little media piracy systems the way they have been for the last 20 years.

Leo: So the insane paranoia really comes from Hollywood, not from Microsoft.

PETER: It's hard to tell what goes on inside Microsoft. But if you read the technical specs, I think any technical person that reads those specs would say this is never going to work, and half of the stuff is nuts. On the other hand, it could well be high-level managers inside Microsoft who don't understand the technology and who completely agree with Hollywood and who think we should do this even though other people have told me it's impossible, we're going to do it anyway.

Leo: You made such a good point, Steve, when you said that they're doing this for a subset of PC users, far from the majority of PC users, and yet we're all saddled with this. In fact, Peter, you say at the end of your document a $50, cheap, Chinese-made set-top player in the long run will do a better job of playing back this HiDef content. Why don't we just extrude all of this extraneous material from our PC and get it out of there? We don't need it.

PETER: Right, exactly.

Leo: Why are we trying to turn the PC into a HiDef media device?

Steve: So I guess the point that Peter is making overall, I mean, his paper was talking about the cost of Windows Vista content protection is that we know that Vista is going to be selling, starting next month, in February of '07. We know that people buying new machines are going to have Vista on it. So we know that a year later there's going to be a huge install base of Vista. We know that there will be people wanting to upgrade their XP systems which are strong enough to run Vista, to have the latest and greatest. And maybe this will sort of mute that enthusiasm for upgrading to some degree, depending upon the kinds of things people do. So this is going to happen anyway. But in order to implement all the technologies Microsoft has, it really does insert cost throughout the entire infrastructure. The whole Windows PC infrastructure becomes more expensive.

PETER: Right. Well, the scary thing is it's not just Windows because the hardware manufacturers have to make these changes, and they don't really care what operating system it's going to run on. It's going to affect everybody. Your graphics cards will become more expensive across the board, even if they're never used with a Windows PC, because they still need to have these changes made only for Windows Vista.

Leo: So really it's interesting, I mean, you could say let's take this out of Windows. But in fact by just putting it in Windows it's now in everything we use.

PETER: Right. Because, again, if Windows – if they own, I don't know what, 90, 95 percent of the market, the graphics card and sound card manufacturers have to handle that. And so they have to put this Vista-specific stuff in there, even if Mac OS X or Linux or FreeBSD completely ignores it.

Leo: We'll put a link to Peter's article, of course, on our web page. It's a long URL, so I'm not going to give it out on the air here. But you can go to our show notes and read it. And I do recommend reading it. As technical as it sounds, it's easily read and digested, I think.

Steve: Leo, has John Dvorak weighed in on this issue at all yet? Have you heard from John?

Leo: No, in fact, we'll probably talk about it more – we're going to get – actually we're trying to get a rebuttal from Microsoft on Windows Weekly and find out what they have to say. I don't expect anything substantive from them, but we want to at least give them a chance to say something. And I think it's pretty clear that the proof will be in the pudding. I mean, as Vista comes out in the marketplace, if all of these things happen as Peter has predicted – and I see no reason why they won't. But if this all happens, you're going to see rebellion. You might be right, Peter, this might in fact be a suicide note because nobody wants their computer bricked. That's the new term we're all going to have to learn.

Steve: And I think Peter made a real good point, too, which has been on my mind, and that is, when you look at all the effort Microsoft has gone to to protect us from Hollywood, or Hollywood from us...

Leo: That's protect Hollywood from us.

Steve: Whichever way it goes. Imagine if instead they had put that industry into protecting us from spyware and malware.

Leo: Well, they'd have done the job, I'm sure. I think ultimately the consumers will be the voters on this one. And they'll vote with their dollars. I have to think, if I'm a business guy thinking about moving to Vista, and I see this, I'm going to have some real second thoughts because there's no benefit at all to business. Business doesn't want HD content on their computers.

Steve: Now, Peter, if you don't have drivers – from the business model, if you had a basic PC with no HD-DVD drive and drivers, security-certificated drivers, no fancy graphics card that had all this stuff, would Vista's content protection system just sort of never get activated? Is it in there, but just completely passive, and there's no tilt bits that are going to be a problem?

PETER: I think probably the nastier aspects probably wouldn't be activated. Again, the specs are vague on just how much of the stuff is actually active at any one time. Because a lot of it is so deeply built into this OS, I think a large chunk of it is probably going to be there no matter what. And that's deliberate. Obviously, if you have one version of Vista that doesn't have the content protection active...

Leo: I'll use that one, yeah.

PETER: ...and a different version of Vista that does, everyone's going to use the unencumbered version.

Leo: You have to put it in all of them.

Steve: Well, in fact I have read through the Vista Output Content Protection document. And it's very clear, exactly what Peter was saying from an architectural standpoint, whole huge subsystems have been completely redesigned and moved around from, like, kernel mode to user mode, and there's this whole notion of a protected environment now to keep things from working the way they have before. So there will certainly be side effects of those kinds of deep architectural changes that we wouldn't have needed except that Microsoft decided they wanted to do this.

Leo: Well, and you have to wonder if that's why Vista took so long. I mean, this attention to this kind of stuff didn't happen until a few years ago. I can imagine Microsoft sitting in 2004 saying, okay, Vista's ready to go, and hearing from Hollywood, well, hold on there, guys. And imagine, it would have taken a year or two to get this stuff working right.

Steve: Well, and in fact historically we've seen that a lot. I was talking last week about how the fights over the content protection for digital audio tape, DAT tape, it delayed its introduction into the consumer market by many years. And people who know about the industry feel that it may have been all of that that just killed it, and it just never had a chance to happen.

PETER: But we've also been getting lots of complaints from people, admittedly running beta versions of drivers for Vista, that the drivers are less functional than the XP drivers, they're less stable and so on and so forth. Lots and lots of complaints. And I know from sort of off-the-record comments from people working for device manufacturers that they're putting a huge amount of effort into getting all this content protection stuff into their device drivers. And they're frantically trying to get drivers out in time for the Vista...

Leo: Must be driving them crazy, yeah.

PETER: Yeah, it's driving them nuts. And obviously they're not getting any value out of this. For some large graphics manufacturer like ATI or NVIDIA, they're getting absolutely nothing out of putting all this crippling into their own drivers. But they have to do it because Microsoft has said so. And so typically with, let's say Windows XP, it's got a pile of built-in drivers. Well, with Vista the release to manufacturing, a lot of the drivers weren't ready yet at the time that was released. So probably the first thing that happens once you install Vista is you have to go online and download drivers that actually work.

Leo: Or support this HiDef content protection.

Steve: Well, and in fact I've been running Vista now for several months. And I don't use it continually. But when I do fire it up, almost all the time it says, oops, there's some new updates ready for your machine, go get them.

PETER: Right. And you can see that, even with playing back non-protected content, in online forums you see complaints about it dropping frames and audio stuttering and so on and so forth. Maybe it's just because it's beta drivers. On the other hand, it could also be because all this content protection gunk is getting in the way of simply playing back the content.

Leo: Peter, you're a little bit like Paul Revere. I don't know if you know the story of Paul Revere in the U.S. saying "The British are coming, the British are coming." Vista is coming. And really it's only until it's out in widespread use we'll really know what the true consequences of this decision on Microsoft's part are. But I have a feeling there's a lot more to be said about this, and we'll be hearing a lot more about it in the months to come. We thank you so much for joining us on Security Now!.

PETER: Okay, you're welcome.

Leo: Really great to talk to you. Thank you, Peter.

Steve: Thanks, Peter.

PETER: Thanks.

Leo: Peter Gutmann, again, who is at the University of Auckland in New Zealand, a well-known security expert, and a guy who has really stirred up a hornet's nest. And we haven't heard a lot from Microsoft about this.

Steve: These are good hornets, Leo.

Leo: These are angry hornets, but it is really a good thing for him to talk about this. I have some concern because, A, this is his opinion, although pretty factually backed up. We haven't heard from Microsoft on...

Steve: Leo, I have read all the Microsoft docs. I have read all of the AACS docs. Certainly Peter is taking the approach of this is a bad thing, an expensive thing for Microsoft to have done. But I can independently vouch for the factual accuracy of what he has said. This notion of them saying that the screen should be made fuzzy if it's not protectable, that outputs need to be shut down, I mean, I have read that myself in documents directly from Microsoft's site. So all of this stuff is absolutely accurate.

Leo: We'll see. Of course it's accurate. I'm not denying that in any way. I just think we won't really know what the price for this is for a few months. But I think it will become clear. The question is, what are we going to do about it?

Steve: Well, and Peter made some great points. He's been very active out in the blogosphere, and certainly he's been the focus of this because of his paper. And he talks about, and I have also seen separately, people saying that something seems wrong with Vista relative to its ability to robustly play media. That is, they play back media. So it may be it's going to take a while for Microsoft to get this working smoothly, and that they've broken it in the meantime.

Leo: Steve, always a great pleasure. You can find more details, including a transcript of this great conversation, at GRC.com. I'm going to Digg this show so that people can – I think this is the kind of thing that people on Digg and Slashdot will want to know more about. Peter hasn't done a lot of interviews, so it's a chance to really hear it directly from

Peter Gutmann. You can help us by going to Digg.com and Digging the story. And if you want more information, as I said, transcripts, 16KB versions, notes, they're all on Steve's site, GRC.com. That's not the only thing there, though. That's where you also find SpinRite, which is Steve's fantastic program for hard drive maintenance and recovery. It was funny that you initially talked to Peter about hard drives.

Steve: Yeah, exactly, because our paths have crossed in many different venues.

Leo: Lots of happy customers. You can go to SpinRite.info to read the testimonials. I think that will tell you more than anything Steve or I could say about the value of the program. If you've got a hard drive, you really ought to get SpinRite. GRC.com. Okay, Steve.

Steve: Well, Leo, another week, another episode is in the can.

Leo: It is.