Microsoft on Vista DRM

Description: In episode #74 Peter Gutmann shared his concerns and fears about the system-wide consequences and impact of the digital rights management (DRM) Microsoft has built deeply into Vista. Microsoft's Vista Team responded with a comprehensive Blog posting which Steve and Leo read and examine this week.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-077.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-077-lq.mp3

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

Leo Laporte: This is Security Now! with Steve Gibson, Episode 77 for February 1, 2007: Microsoft Responds.

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

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!, everybody's favorite security podcast. And here he is, ladies and gentlemen, the star of our show, Mr. Security himself, Steve Gibson. Hey, Steve.

Steve Gibson: Hey, Leo.

Leo: We need a live studio audience with music. It'd be fun to do all that.

Steve: Whistles and catcalls and things, yeah.

Leo: So we are going to address a podcast that we did a couple of episodes ago this week.

Steve: Right. I wanted to, in all fairness, I wanted to give Microsoft's response to Peter Gutmann's white paper about Vista DRM some airtime. I was thinking we could just tell people to go to this link. But it's like, wait a minute, this is an audio podcast, let's audio-ize Microsoft's publicly posted blog response and discuss it. Because, you know, obviously Microsoft was not happy by what Peter had to say.

And so what happened was David Marsh, who is the guy whose name I've seen on all the documentation on all of the PowerPoint slides that are presented, he's the guy at the WinHEC conference who exposed this for the first time, showed what AACS was, how it works, I mean, he's the main guy at the center of Vista's support for AACS. And some guy named Nick White, who's with the Vista team, he has a Vista Team Blog. On Saturday January 20 he posted, essentially asked Dave to come up with 20 questions and answers which – basically synthetic questions which Dave felt were being raised by Peter's white paper, and to address those, to answer those questions.

In going through them, what I'm going to suggest is that you read this, Leo, and then I'll sort of react to them and tell you what I think about them. And many of the points are very fair. And I think we're most useful to our Security Now! listeners if we really work to paint a balanced picture. Certainly it's been fun to look at the sort of, okay, what's the dark side of AACS. But many people are wanting to use Vista. They're going to use Vista. Many are going to have to use Vista. Or when they're buying a new PC, it'll have Vista on it, and they may not have a choice. So I want to back off from overstating and also give Microsoft a chance to tell their side of the story.

Leo: So in this particular podcast I'll play the role of Microsoft. I'm Dave Marsh. And shall I just start reading, and you stop me when you have something to say, how about that?

Steve: Yeah, I think that's perfect.

Leo: Dave begins: Over the holidays, a paper was distributed that raised questions about the content protection features in Windows Vista. The paper draws sharp conclusions about the implications of those features for our customers. As one of the lead program managers for the technologies in question, I'd like to share our view on these questions. Windows Vista – anything from the opposition? Nothing, okay.

Steve: No.

Leo: Windows Vista includes content protection infrastructure specifically designed to help ensure that protected commercial audiovisual content such as newly released HD-DVD or Blu-ray disks can be enjoyed on Windows Vista PCs. In many cases this content has policies associated with its use that must be enforced by all playback devices. The policies associated with such content are applicable to all types of devices, including Windows Vista PCs, computers running non-Windows operating systems, and standalone consumer electronics devices like DVD players. If the policies required protections that Windows Vista could not support, then the content would not be able to play at all on Windows Vista PCs. Clearly that isn't a good scenario for consumers who are looking to enjoy great next-generation content experiences on their PCs.

Steve: Now certainly he raises the point, basically he's trying to say we didn't create this, we didn't do this. And if we didn't offer this kind of DRM content protection, then Windows Vista PCs would not be able to play it. And that is absolutely true. I mean, it is the case that the way AACS works is that the content providers, through this really super-powerful, next-generation DRM, this digital rights management, they're able to absolutely dictate what devices are able to play. So it's only if Microsoft provides an infrastructure, which they have with Vista, which is sufficiently secure and provably secure, that then there's any possibility for Windows machines playing this content.

Leo: So it's really basically what a number of rebuttals to Peter's argument in Peter's own website said, hey, they don't have a choice, they have to do it.

Steve: Right. Essentially all Windows Vista is is another implementation of AACS, much as you will have in any consumer device. There will be AACS there if that device is able to play this AACS-protected content.

Leo: Peter made an argument, frankly, an argument for which I don't think he has any standing, saying, well, hey, Microsoft could have just said, we're Microsoft. We have 90 percent of the PC market; we're not going to do it. I mean, that's a business argument. It has nothing to do with security. And I don't know if any of us are competent to say whether Microsoft could or could not do that. Maybe they should, but...

Steve: Well, but Microsoft, yeah, if Microsoft had done that, we then are faced with the question, would hi-def content providers essentially have scrapped all their content protection because they're so desperate to have movies playable on personal computers? I think it's clear that that's not the case, that content providers would say, fine. If you are not going to give us a secure platform, Windows users – XP users, Vista users, any users – just like, by the way, Linux users, and I don't know where Mac is on this. But, for example, Linux users are not able to play hi-def content either because Linux doesn't bring all of this protection that's necessary. And we are seeing the danger in XP users being able to play this, as we talked about last week, this muslix64 character is using now a known plaintext attack on the 'cryption used with this content. So again, if Microsoft had said, we're not going to play ball, then I think it's very clear that Windows Vista would not be able to play hi-def content.

Leo: So I will continue on here. Associating usage policies with commercial content is not new to Windows Vista or to the industry. In fact, much of the functionality discussed in the paper has been part of previous versions of Windows and has not resulted in significant consumer problems, as evidenced...

Steve: Okay, now, stop there.

Leo: Whoa, whoa, whoa.

Steve: In fact, much of the functionality discussed in the paper has been part of previous versions of Windows.

Leo: That's not true.

Steve: That's absolutely not true. I will defend David's need to have this in Vista because there's no other way, if Vista's going to be able to play HD-DVDs. He cannot say that much of the functionality discussed in the paper. Because, I mean, the paper was all about the bad parts of DRM in Vista, none of the happy news. So it's...

Leo: He could say, okay, so there was a random number generator. I mean, I guess you could say some sort of root technologies were there. But there wasn't an AACS layer.

Steve: We had no tilt bits, and we had no encrypted video path and all that other stuff, no. So, I mean, I'm sorry.

Leo: He continues on: ...as evidenced by the widespread consumer use of digital media in Windows XP, in other words, no consumer problems. For example, standard definition DVD playback has required selective use of Macrovision ACP on analog television outputs since it was introduced in the 1990s. DVD playback on and in Windows has always supported this. I guess he's saying earlier generation forms of copy protection, like Macrovision. He also goes on to say: The ability to restrict audio outputs, for example S/PDIF for certain types of content, has been available since Windows Millennium Edition and has been available in all subsequent versions of Windows. Oh, that's interesting. I didn't know that.

Steve: Yeah, I didn't know that.

Leo: The certified output protection protocol, COPP, was released over two years ago for Windows XP and provides applications with the ability to detect output types and enable certain protections on video outputs like HDCP, CGMS□A, and Macrovision ACP. So he 's pointing out, look, there's been copy protection technologies in Windows all along.

Steve: And they haven't been a big problem for consumers.

Leo: Nobody's blown their stack saying my S/PDIF won't work because – although Macrovision has caused problems all along. But...

Steve: Oh, and it always will. I mean, it's just a yucky analog technology that messes up what should be a good video signal.

Leo: You can't really say people aren't upset about Macrovision. He goes on – I'm again quoting, just so this is clear this isn't me talking, this is Dave's response. Dave Marsh is the lead program manager for Windows video handling, and this is his blog response to Peter Gutmann's article. He goes on to say: It's important to emphasize that, while Windows Vista has the necessary infrastructure to support commercial content scenarios, this infrastructure is designed to minimize impact on other types of content and other activities on the same PC. That was one of Peter's big contentions is that the whole PC suffers for this. For example...

Steve: I have to say, Leo, that anecdotally we are – we don't really know why yet, but people are reporting Vista is not as good a media platform as XP. I've seen a lot of posts in my newsgroups and elsewhere where someone has upgraded themselves to Vista, got it all running, done some stuff, just playing non-protected content on Vista, and the picture stutters, it's jerky, it's not looking nearly as good as XP was. Then they'll fall back to XP, and it's working much more smoothly. So, I mean, it may very well be that there is some impact to this, unfortunately, even when playing non-protected content. And it's going to be systemic throughout all of Windows Vista.

Leo: I should, to be fair, point out it could just be suboptimal drivers. Now, Vista is just now out. But Microsoft's been optimizing drivers the entire time since December or November when Vista RTM came out. So it could very – there are lots of reasons for it. I

think it's early to say what the case is, whether it's a problem or not. He gives an example: If a user were viewing medical imagery concurrently with playback of video which required image constraint, only the commercial video would be constrained, not the medical image or other things on the user's desktop. Similarly, if someone was listening to the commercial audio content while viewing medical imagery, none of the video protection mechanisms would be activated at all, and the displayed images would again be unaffected.

Steve: And of course that was one example that Peter gave of somebody listening to protected audio, some medical image processing guy who was – and Peter was concerned that the fact that there was – he said that the system was all or nothing, was his reading. And I'm sure Peter believed that that was the case. So I think this is a case of a clear mistake in the way the system works, understanding the documents. I have to say, too, that from what I saw, what Peter stated was entirely believable and reasonable. So David is putting to rest that concern that, if any protected content is anywhere in the system, then the whole system locks itself into paranoia mode and makes the screens blurry and so forth. Clearly that's not the case.

Leo: Well, as anybody who has ever read specs and designed software will absolutely agree with, the software doesn't always reflect what the specs say. It may have been the intent; it may have not been the intent. But it's perfectly possible that the documents read one way and the software does something else.

Steve: That's a very good point.

Leo: Contrary to claims made in the paper, the content protection mechanisms do not make Windows Vista PCs less reliable than they would be otherwise. If anything, they have the opposite effect, for example, because they will lead to better driver quality control.

Steve: Certainly at best that's an unsupportable statement.

Leo: It's a spin. It's a spin, let's face it.

Steve: Yeah, I mean, that one's really hard to get behind. Certainly we're talking about much more complexity. It is the case, though, that certain classes of mistakes, that is, the sorts of mistakes that would lead to a driver leaking content, that's something that any driver author will have a real concern not to allow to happen. So, I mean, basically Microsoft through this is raising the stakes on errors by forcing driver makers to make sure that they just – essentially creating a much greater penalty if there is a problem. So you could say, well, that's going to lead to better drivers. It's like, well, let's let history determine whether that's the case.

Leo: It could also lead to more crashes. We just don't know yet. It's like, you know, we've raised our standards. It's not exactly what they were doing, they're saying we're making it much less tolerant of faults.

Steve: Yeah, well, now, I was just going to say, we have these tilt bits all over the place. And it's like, well, let's hope those don't go off.

Leo: Going on to quote Dave: The paper implies that Microsoft decides which protection should be active at any given time. This is not the case. The content protection infrastructure in Windows Vista provides a range of a la carte options. It allows applications playing back protected content to properly enable the protections required by the policies established for such content by the content owner's service provider. In this way the PC functions the same as any other consumer electronics device. With that introduction, here are the top 20 questions and answers. So we'll go on to those.

Steve: Yeah. I think that's fair. Although I have to say I did not read what Dave is suggesting in Peter's paper. He says the paper implies that Microsoft decides which protection should be active. I didn't get that impression. So he's disabusing us of something that I don't think Peter said. I think it's very clear that Microsoft facilitates whatever protection the content provider wishes to have.

Leo: This is what an operating system provider does. They provide a platform with the technologies that are required. And then the playback device decides which ones it wants to take advantage of.

Steve: Exactly.

Leo: All right, now. This is probably where you wanted me to start reading. But anyway...

Steve: No, no. I'm glad we did that. I'm glad we have a foundation there. And so we have 20 questions and answers. And I have to just say that I've read all this already. And I think we'll see that some of these questions are questions Dave wanted to ask so that he could answer them. They're not necessarily things that a fair reader of Peter's paper would have come away believing or being concerned about.

Leo: All right. Question 1. So again, Dave Marsh, this is him posing a question: Do these content protection requirements apply equally to the consumer electronics industry supply player devices, such as an HD-DVD or Blu-Ray player? The answer is: Generally the requirements are equivalent for all devices. For example, an HD-DVD or Blu□ay disk always requires HDCP protection for the DVI HDMI outputs, regardless of the type of device playing the disk. There are some cases, such as DVD video, where PCs have slightly different protection requirements than CE devices. But these differences are mainly historical and as dictated by the licenses associated with the systems providing access to the content. For example, CSS for DVD. So he's saying basically yes, they have the same requirements.

Steve: Yes, and I think that's completely fair. Essentially, Windows Vista becomes an HD or Blu-ray hi-def content player, just like you could buy off the shelf.

Leo: The subtext is, hey, we're just like everybody else. We're just doing what we have to.

Steve: Exactly.

Leo: Question 2: When are Windows Vista content protection features actually used? He answers: Windows Vista content protection mechanisms are only used when required by the policy associated with the content being played. For Windows Vista experiences, if the content does not require a particular protection, that protection mechanism is not used.

Steve: And I think that's, again, very fair and a balanced appraisal. It's not like Microsoft is adding DRM where it didn't exist before. And they're not basically constraining the channel that the content provider has not required be constrained. And part of the power and flexibility of AACS is that there is such a strong capability for usage policy to be bound in with the content. And so again, Vista is just being a fair playback device. And if it weren't, it wouldn't be allowed to be a playback device at all.

Leo: Right. Makes sense. Is this question three? Yeah, Question 3: Will the playback be reduced on some video output types? Image-quality constraints, David says, are only active when required by the policy associated with the content being played, and then only apply to that specific content, not to any other content on the user's desktop. This is that medical imaging example.

Steve: Exactly.

Leo: As a practical matter, image constraint will typically result in content being played at no worse than standard definition television resolution. In the case of HD optical media formats, HD-DVD and Blu-ray, the constraint requirements is 520K pixels per frame, i.e., roughly 960x540. That's still higher than the native resolution of content distributed in the DVD video format. We feel this still yields a great user experience, even when using a high-definition screen.

Steve: I think, again, that's an absolute fair and accurate rendition of what's really going on. You can imagine that a laptop user who had a HD-DVD drive in his laptop, you know, buys it because he wants to be able to watch movies on his laptop. And so he would have to have Vista. He would not be able to do this with XP because XP doesn't provide this. So Vista integrated in with a laptop that's got an integrated LCD screen and drive, it's simply going to be an HD or Blu-ray DVD player. It's going to work.

Leo: Actually a little better because it's 520P instead of 480P.

Steve: Exactly. I mean, not substantially, but a little bit, yeah. Well, and actually...

Leo: But that's not what Peter asserted. Peter was saying it would really go down in quality below 480.

Steve: No, actually I think Peter was talking about the 520K pixel a frame. He just didn't like the idea that there was this artificial constraint imposed by Windows. And again, Dave is saying, wait a minute, this is not our imposition. And it's true that, again, the content provider says, if you're not going to provide digital encryption all the way to the screen, where it finally jumps off the screen and travels by light into the user's eyeballs, then you must provide the following constriction. So again, Windows is simply enforcing the policy that the content provider has bound in with the content. And so, yes, the content provider could say we want it

to look really smeary, 200K pixels or 100K pixels. Again, Microsoft has no control over that. So David is assuming that the content provider is not going to ask for something blurrier than 520K pixels per frame.

Leo: Ah, so they could.

Steve: Yes. We don't really know that.

Leo: Okay. Will this affect things like medical imagery applications? David answers: Image constraints only apply to protected content being played and not to the desktop as a whole. Therefore, the resolution of other non-protected media, such as medical images, is not affected.

Steve: Right.

Leo: Good. That's great.

Steve: So clearly, if you're running your medical imaging utility in a window, and you also have hi-def playing in another window on your screen, the hi-def video constraint may cause that to be blurred, but not a separate window running on the same system which is displaying completely crisp, non-resolution-lowered images. So it's certainly possible for Windows to do that, and David is asserting that's the way it works. I would be surprised if it did not.

Leo: He's actually so adamant in this assertion, I think we can trust that that's the case. Otherwise that would cast this entire document into doubt.

Steve: And there's no reason for it not to be. I've looked at the architecture...

Leo: As long as they can do it. That's the key; right?

Steve: Yes. I've looked at the architecture, and it's clear from their diagrams that they have the ability to just protect a certain path of video through the system, separate from all others.

Leo: Do things such as HFS, Hardware Functionality Scan, affect the ability of the open source community to write a driver? This is another one of Peter's very strong criticisms. David says: No. HFS uses additional chip characteristics other than those needed to write a driver. HFS requirements should not prevent the disclosure of all the information needed to write drivers. Just to recap, Peter said that there has to be some secret sauce in every driver that cannot be opened publicly. That's kind of a requirement of the content protection. So Dave said, no, but you still can expose everything you need to know.

Steve: Yes, exactly. So he's coming at it in the classic sort of black hat/white hat fashion, by which I mean you're able to look at one thing and spin it in two different directions, depending upon what's best for you. So Peter was saying that you cannot completely document the hardware or it would be possible for someone to write a software emulator for that hardware and fake out the system to believe that what they had written in software was actually

protected hardware, where it wouldn't be. And Dave is coming at it from the other side, saying, well, okay, but it is necessary not to disclose everything in order to allow the hardware functionality scan to verify the hardware. But he's saying even though it's necessary not to disclose everything, it's not necessary that everything be disclosed in order to write fully functional drivers. And so I agree with him.

Leo: You have to rely on – as always, if you're going to write an open source driver, you just have to hope that the company that made the hardware is exposing everything you need to know. And that's always been a crapshoot.

Steve: Right.

Leo: Will the Vista content protection – so I guess if a hardware company really wants an open source driver, in other words, they can expose enough information to make that possible.

Steve: Exactly. And they can still keep some things private that will not be part of that open source driver. It will not the hurt the driver's ability to function while still giving them the leverage they need of making sure that their driver cannot be emulated by software.

Leo: He goes on: Will the Vista content protection board robustness recommendations...

Steve: Meaning the AACS, for example.

Leo: Okay. Will the Vista content protection board robustness recommendations increase the cost of graphics cards and reduce the number of build options? He responds: Everything was moving to be integrated on the one chip anyway, and this is independent of content protection recommendations. Given that cost, particularly chip cost, is most heavily influenced by volume, it is actually better to avoid making things optional through the use of external chips. It is a happy side effect that this technology trend also reduces the number of vulnerable tracks on the board.

Steve: Okay, that's another spin.

Leo: That's a big fat spin.

Steve: That's a big spin. He was certainly feeling defensive, that is, Dave Marsh was feeling defensive against the allegation that hardware needed to be changed; that, for example, you couldn't have a hardware board that didn't have some components on it which was leaving traces unused where you might have content leaking out of those traces. Well, my feeling is this is not something that David ought to try defending. I mean, he asked the question, so I guess he wanted to answer it. Unfortunately, his answer is not very convincing in this case. I mean, it is the case that in order to have a system – and this was our original premise, Leo, when you and I first talked about this, is essentially adding AACS and this level of DRM is a heavy impact to Windows. But it's not just software, it's hardware, because of course a deliverable solution is both hardware and software. So if you're going to protect the software, it does no good not to protect the hardware. So Microsoft that only makes the software is trying to defend the need to also protect the hardware. I don't think this is Microsoft's problem. So

again, this is why I don't think David needed to address this. I agree, however, that it would be much more convenient for board makers, just as Peter said, to have the option of populating the boards just as they do now with those components they choose to. I don't know that since everything is moving toward one chip argument really holds at all. So I think we need to sort of discount that one.

Leo: Yeah. It's like Martha Stewart saying "It's a good thing." Will Windows Vista content protection features increase CPU resource consumption? Another contention of Peter Gutmann. As he said, it's going to slow everything down because the system has to 30 times a second be checking for piracy.

Steve: Oh, and not only that, Leo, but if you're using an external video card, as power users want to, that cross-bus encryption, you're needing to encrypt at high-bandwidth rates. That's a huge burden on the system.

Leo: And he says yes. David says output content protections are not new requirements for commercial – I'm sorry. Read the wrong one. He said yes. Same answer. Yes. However, the use of additional CPU cycles is inevitable as the PC provides consumers with additional functionality. Hey, it's additional functionality. You're getting additional functionality. Windows Vista's content protection features were developed to carefully balance the need to provide robust protection from commercial content – I don't think he means "from" commercial content, I think he means "for" commercial content – while still enabling great new experiences such as HD-DVD or Blu-ray playback. Of course, if I don't have an HD-DVD player or a Blu-ray player, is it still going to eat those CPU cycles, even though I can't?

Steve: No. And so here again, okay. First of all, this was a total spin answer. So, you know, sorry about that.

Leo: Well, at least he said yes. At least he didn't deny it's going to use more CPU resources.

Steve: Good point. And there's no way Microsoft had a choice. That is, they had to run encryption at high-bandwidth rate across the bus in order not to allow a bus probe to simply grab the hi-def video. So they're having to encrypt from the driver to the display card hardware across the bus, which requires very high speed. In fact, so high speed that AES, the encryption that's used throughout this, is unable to keep up. Intel had to come up with an abbreviated cascading AES to be fast enough for software to be able to do this on the fly. What I think we're going to find is that a system which is playing hi-def content probably cannot really do anything else. It's going to pin the processor, well, I don't see any way of not saying it's just going to pin the processor. And so that's something very different about not playing hi-def content. So it's not always going to pin the processor. It's only when it's playing hi-def content that requires that the hardware bus be encrypted. That's such a burden on the system, that's probably all you're going to be able to do. On the other hand, that's probably all anybody wants to do. If you're playing hi-def content, you're in movie-watching mode. You're probably not trying to write letters home at the same time.

Leo: Well, you'd better not be.

Steve: And you may not be able to. Or maybe you could do email.

Leo: Although, see, I think part of the contention was it also uses up CPU resources even when you're not watching content. Right?

Steve: No. Well, it really seems like – and that's a little bit in the spec gray area – as though only the things that are required are being brought to bear by Microsoft. And certainly when you're not playing protected content you're not having your bus encrypted because there's just no one asking for it. So it would be nuts for Microsoft to leave this really high-overhead stuff on all the time. Therefore I'm sure they're not.

Leo: It's smart enough to say, oh, well, you're not playing a DVD, so we won't use up your CPU.

Steve: Right.

Leo: Okay. Let's see. Aren't there already output content protection features in Windows XP? I don't think anybody's asking this question, but...

Steve: There's a perfect example of a question that nobody asks.

Leo: He chooses to answer anyway. But wait a minute, aren't there already these things in XP? Yes, he says. Well, really. Output content protections are not new requirements for commercial content. The CSS content protection system for DVD video disks requires output protections such as Macrovision ACP and limiting the resolution on component video outputs on standard definition. Windows XP has supported these requirements for some time.

Steve: Which is really interesting because I have never ever heard of any resolution limitation, I mean, I've never seen an API or a spec or anything that indicated there was resolution constraint happening on component video outputs. That's news to me. I'm going to take Dave at his word because he's the expert on this. But again, nobody was really asking.

Leo: And if you ever ask, we've got the answer. Is content protection something that is tied to high-definition video? He answers: While HD content has some unique content protection requirements, many of the requirements apply to commercial content generally, independent of resolution.

Steve: Okay.

Leo: Who asked this question? And what does it have to do with the subject at hand?

Steve: Exactly, good question.

Leo: What's the point? There must be a reason he brought this up.

Steve: I guess, okay, is content protection something that is tied to high-definition video, the idea being, is this all just about high-definition video? And he's saying, no no no, there's streaming video, there's audio can ask for it, you know, blah blah blah. We're just a big, happy DRM platform. We'll provide it for anybody who wants it.

Leo: Anybody who wants it. In fact, he goes on to ask: What about S/PDIF audio connections? And answers his own question: Windows Vista does not require S/PDIF to be turned off. But Windows Vista continues to support the ability to turn it off for certain content, a capability that has been present in Windows for many years. Additionally, in order to support the requirements of some types of content, Windows Vista supports the ability to constrain the quality of the audio component of that content. In other words, like image constraint.

Steve: Exactly. You're able to make it muddy.

Leo: Similar to image constraint for video, this quality constraint only applies to the audio from content whose policy requires the constraint, not to any other audio being played concurrently on the system. As a practical matter, these audio restrictions are not widely used today.

Steve: So I guess it sounds like the audio could be down-sampled and its resolution limited in the same way that they're able to do with video if that's what the content provider says they want.

Leo: And he does point out, and I think this is important, nobody's doing this. In fact, nobody's doing it in video yet, either, as far as I can tell. So this is all kind of could be, might be. Will component – that's the YPBPR, what is that, chromium red, I can never remember, the blue, anyway, you know which ones we're talking about – the component video outputs be disabled by Windows Vista under content protection? Similar to S/PDIF, Windows Vista does not require component video outputs to be disabled, but rather enables the enforcement of the usage policy set by content owners or service providers, including, with respect to output restrictions, an image constraint. So...

Steve: So he's saying, it's not our fault that we allow S/PDIF to be disabled.

Leo: Or component.

Steve: Yes, component or S/PDFI, right. Where, you know, it's not our fault that we allow it to be turned off. We have to make it disable-able in order to satisfy the demands of the content providers. So again, they're just sort of being the middleman between the content providers and the end user. Which, you know, is fair.

Leo: Sure it's fair.

Steve: Yeah. If you want that sort of thing.

Leo: If you want that sort of thing. Will echo – actually that's really probably for things like set-top boxes. Cable companies might turn off component and force you to use HDMI if you're watching HD content, things like that.

Steve: Yeah, exactly.

Leo: Will echo – so I guess Windows Media Center would have to do the same. Will echo cancellation work less well for premium content? We believe – I don't even know what echo cancellation is. We'll find out. He responds: We believe that Windows Vista provides applications with access to sufficient information to successfully build high-quality echo cancellation functionality. What's he talking about?

Steve: The reason this is an issue is that the way echo cancellation functions is by feeding back into the echo cancellation circuit some of the output. You feed it back in, sort of like 180 degrees out of phase, in order to cancel it sending itself back up the line. Peter made the point that, if audio was being constrained, then the echo cancellation system would inherently be less effective because it wouldn't be able to perfectly match essentially the echo signal which it would otherwise be. And so David is saying, oh, don't worry about it, it still works. It's like, okay, we'll see.

Leo: I didn't know that.

Steve: And also it's worth noting that, if what Microsoft is saying, and that there would be audio constraint for protected content, one wonders why you would ever have echo cancellation happening to protected content. You would typically have it for VoIP, for example. When two people are talking you want echo cancellation so that you're not hearing yourself coming back the other end. But a normal dialogue between people over a VoIP call, that's not going to be protected content. Therefore there would be no artificial constriction to the audio. So I do think that Peter was raising a theoretical point that would in fact never affect anybody in the real world.

Leo: That makes sense. Will it mean there will – this is actually a direct response to a statement in Peter's article. Will it mean there will no longer be unified graphics drivers? Peter said that's it for unified graphics drivers. Here's David's response: The Windows Vista content protection requirements for graphics drivers will not lead to movement away from unified drivers. In fact, all graphics drivers shipped with Windows Vista are unified drivers. Well, there you go.

Steve: I mean, it's interesting, though, because remember that Peter's point was, if you had a single driver which covered a broad range of cards with different capabilities, if a HD card were found to need its driver revoked, since you had a unified driver, then you would be revoking a huge set of cards. That is, you'd be revoking all drivers because you had a single unified driver that was covering your whole line of cards. So he was saying this would force manufacturers to do per-card drivers rather than unified drivers. So I don't think Dave has really addressed that issue at all. He says, well, Windows Vista is using unified drivers, and they're just fine. It's like, yeah, well, let's hope that none of them are ever revoked. Because then whole families of cards will die en masse.

Leo: So he's not saying there's no technical reason you can't do a unified graphics driver. It's just it might be a good idea. Apparently Microsoft doesn't think that's ever going to happen, this mass revocation.

Steve: It really does sound like that's the case. Or, and I think we'll see that if they – they're hoping and assuming they would always be able to replace a driver that is soon to be revoked with a new driver that would have then different keys and would fix the problem that went wrong with the bad driver. So essentially the replacement would arrive before the revocation of the prior version.

Leo: Okay, right. So in other words – yeah, okay, right. You get a new version before they make your old one not work.

Steve: Yeah.

Leo: Will Windows Vista audio content protection mean that HDMI outputs can't be shown as S/PDIF outputs? Will Windows Vista audio content protection mean that HDMI outputs – HDMI carries audio – can't be shown as S/PDIF outputs?

Steve: Apparently in the UI it actually shows the HDMI video...

Leo: Looks like S/PDIF.

Steve: Exactly.

Leo: Okay. Dave says: It's better if they show as different codec types as it allows the difference to be reflected in the UI, thus providing the user help with their configuration and creating a better user experience.

Steve: The user...

Leo: Yeah, wants to know the difference between HDMI and S/PDIF as they are different physical connectors.

Steve: Okay. I don't know why we care about this one.

Leo: I don't even know. Maybe he's – I don't know. Okay. Next question. What is revocation and where is it used? Now, here's a good question. Dave responds: Renewal and revocation mechanisms are an important part of providing robust protection for commercial audiovisual content. Sounds like he's quoting the MPAA. In the rare event that a revocation is required, Microsoft will work with the affected IHV – that's the hardware guy, the guy who built the card that's going to be revoked...

Steve: Independent Hardware Vendor; right.

Leo: ...to ensure that a new driver is made available, ideally in advance of the actual revocation. That's what you were saying.

Steve: Exactly.

Leo: Revocation only impacts a graphics driver's ability to receive certain commercial audiovisual content. Otherwise the revoked driver will continue to function normally. So your card still works. You just won't be able to watch HD DVDs.

Steve: Now, that's huge big news because that's a really important point that I want to make sure everyone got is that Peter's paper – and we all just kind of went along with it without thinking about it – presumed or stated that the driver would be revoked, and all of those drivers would no longer function. And David is saying, whoa, no, all we're doing is we're revoking the hi-def capability of the driver. You can still watch non-hi-def movies, even, and your desktop will work, and everything else will work. I mean, it's like, when you hear it, it's like, oh, duh, of course that's the way it would and should work. So it's not like no one's computers are going to work anymore. It's just that, if there isn't a replacement already on your system, and you are hit with revocation, you lose the ability to play hi-def content. You don't lose anything else about your driver's ability to function. Which I think is, again, a really important point to make.

Leo: And of course we've said a couple of times it doesn't seem likely that revocation will ever happen. However, you can't assume it's not going to. It's built in, so you have to assume at some point they're going to use it.

Steve: It's in there. It's in there.

Leo: There's also the issue of what if – and this Peter raised, and I don't see it, maybe we'll get to it. It sounds like you have to continue to pay your dues to this organization, whatever organization's doing this, to continue to be certified. In other words, you could be revoked, not because you cracked content protection, but just because you didn't pay your dues. Which means, if you went out of business...

Steve: That's bad.

Leo: ...you could be revoked. But the good news is revocation, at least according to Dave, doesn't mean the thing stops working, it just means you can't play high-end content.

Steve: And I think it's another perfect example of a nightmare scenario that's very unlikely to occur. Certainly the MPAA or the content provider, the AACS organization, they could revoke anyone's licenses they wanted to at any time. I would be surprised if somebody choosing not to renew their license would automatically force the revocation of their earlier license. I mean, that's, okay, they have the capability to do so. I think it's a real stretch to presume that they therefore would. I think somebody could just say, we're going out of business, we've got 100,000 graphics cards out there. As long as those aren't breached, then I would imagine they would continue to function. The danger would be if revocation was then necessary, the manufacturer was out of business, Microsoft did not have the source code in order to fix the driver themselves, and then users of those cards of the company that went out of business

whose drivers were revoked for playing hi-def content, they'd be in bad shape.

Leo: It may not be so academic. I think because of muslix64's work, it may well be that some of these keys get leaked out and revocation – we'll see. It's going to be just a matter of time before keys for some of these cards are leaked out. Explain this to me, but this is how I understand it, that each video card or playback mechanism has its unique key. And in order to use the AACS unprotect software that muslix has written, you need the key for the card you have.

Steve: A simplified way of describing it is as follows: Imagine that there's a universe of keys that will ever be used. And so the title's decryption key is encrypted with every different key possible, and it's put on the disk. So what happens is your player decrypts its specific matching key, which is on the disk. And that allows it to determine the decryption key for the title. But if the disk no longer contains an encrypted version of the key for the player's key, then there's no way it can decrypt the title key. That really didn't simplify anything, did it.

Leo: Well, okay, so...

Steve: Now everyone's confused.

Leo: No, that made sense. So let's talk practically. So in order to use muslix64's unencryption technique you have to get the key for your playback device. Let's say somebody online starts distributing these keys. Now, nobody has yet, at least to my knowledge. I'm sure in some private areas they are. But let's say these keys start getting distributed. Now, at that point, wouldn't these keys get revoked?

Steve: Yes. Well, those particular disks are now forever cracked. That is, you can certainly imagine that there will be a cracking site that will start listing the decryption keys for all the disks that have been cracked.

Leo: So they're giving out keys for the disk, though, not for the hardware.

Steve: Yes, and what's called the "title." It's called a "title key."

Leo: But it doesn't have to match your hardware card.

Steve: Well, exactly. Then the title key would allow you to decrypt the digital content and then play it anywhere you want.

Leo: On any device. Okay, so this is...

Steve: And the title keys are already leaking.

Leo: Yes. I shouldn't have brought this up, then. This doesn't have anything to do with the

hardware revocation.

Steve: Right.

Leo: Well, okay. Going back to revocation, he says: Does this complicate the process of writing graphics drivers? In other words, kind of dividing the premium content playback into a separate section that can be revoked from the regular content playback, which cannot be revoked. Dave responds: Adding new functionality usually introduces new complexity. In this case, additional complexity is added to the graphics driver, but that complexity comes with the direct consumer benefit of new scenarios such as HD-DVD or Blu-ray playback. Basically the answer is yes.

Steve: Yes. It's going to be more complex, but it had to be.

Leo: It had to be. You're playing back new content. But it does mean that the hardware manufacturers and the driver authors are going to have to be aware of this, cognizant of this, to keep their cards working after revocation, should revocation happen.

Steve: Yes, good point.

Leo: Question: Will the tilt bit mechanism cause problems even when the driver is not under attack from a hacker, for instance there are voltage spikes? And this is something we really talked about with Peter. Voltage fluctuations are a constant in the PC hardware world. Wouldn't that set a tilt bit? Dave answers: It is pure speculation to say that things like voltage fluctuations might cause a driver to think it's under attack from a hacker. It is up to a graphics IHV – manufacturer – to determine what they regard as an attack. Even if such an event did cause playback to stop, the user could just press Play again and carry on watching the movie after the drivers reinitialize, which takes about a second. Now, remember that these tilt bits are set 30 times a second; right?

Steve: Yes, every 30 milliseconds there's a scan done.

Leo: Basically you could be pressing that spacebar a lot. Okay. Again, it is important to note that this could only occur in the case of watching the highest grade premium content such as HD-DVD or Blu-ray. In practice I doubt it would ever happen. Well, we don't know.

Steve: And we're not going to know until – it would be annoying if it took you three hours to get through a two-hour movie.

Leo: You'd have to keep pressing the spacebar.

Steve: That would be a problem. Time to get a new power supply.

Leo: It seems like a card manufacturer would try to avoid that particular scenario.

Steve: Especially now that it's had so much attention. They're not going to have any tilt bits on their power lines.

Leo: Right. But there may be other issues. All right. I'd love to hear what Peter said about this one because I got the strong impression from Peter that that's the kind of thing cards have to look for. That kind of voltage modulation is one way hackers might attack these disks.

Steve: Well, I think, frankly, I think what Peter was offended by from a purist standpoint, the idea that Windows requires maximum robustness in order to survive out in the real world anyway, that you're going to have voltage fluctuations, you're plugging USB and Firewire devices in, you know, it's like there's just a lot going on. And so Windows needs every benefit of the doubt in order to be as reliable as it is. And so what this does is this deliberately removes every benefit of the doubt so that if there is any doubt, a tilt bit gets set, and Windows resets its whole graphics display system. So again, we won't really know until this has been out for a while. And I think Peter was mostly concerned about the idea that, rather than – that we're switching from a benefit of a doubt to allowing no doubt whatsoever.

Leo: Right. You know who I'd really love to hear from and who could best answer these last few questions is a video card manufacturer. I mean, they're the ones who have to deal with this in the real world.

Steve: And in fact Peter quotes ATI throughout his presentation, talking about all of the cost which gets passed on to the consumer. That was a big issue in his original white paper was that, yes, this is all more complex, no more unified drivers, no more unified hardware. It's going to raise the cost to the consumer, especially having to do massive sorts of decryption in the hardware of the card itself now, if it's going to be a plug-in card on a bus.

Leo: Another question. Does Windows Vista's use of OMAC□authenticated communication impact graphics driver performance? Dave answers: The authenticated communication mechanisms used for protected video path in Windows Vista are only actively used while commercial content is playing. That means that, while there's a performance impact, it's limited to the scenarios where it's required to provide robust protection for commercial content. Just as you said, it ain't gonna slow you down unless you're watching a hi-def movie, and in that case, what the heck are you doing doing anything else?

Steve: And given what we know now, it's probably going to slow you down a lot. But again, it's going to suck up...

Leo: It's busy.

Steve: It's very busy. It's very busy.

Leo: I'm working here. Do content protection requirements mean that graphics chips have to provide hardware acceleration for video decode? Dave says: No. The Windows Vista content protection requirements do not require that graphics hardware include hardware acceleration for decode for many years. But such support is highly recommended to improve the user experience for HD content.

Steve: Again, this is one where it's not – Microsoft's trying to defend something which is really not theirs to defend. The answer is certainly yes. The more power your graphics card has, the less power you need from the rest of the system in order to do your decoding. So but again it's hi-def itself which is going to be a substantially greater burden on the system than playing a standard YouTube video in a small window, which is just not going to take much of your system's power. So again, it's Microsoft sort of saying, defending something that's really not their problem, but which is just a consequence of a PC being turned into a hi-def media platform.

Leo: Right. Again, I don't know if anybody's been asking that question, but now we know the answer.

Steve: I don't think so.

Leo: Will the video and audio content protection mechanisms affect gaming on the PC? This might be the question I hear most often asked. Dave says: The Windows Vista content protection features were designed for commercial audiovisual content and are typically not used in game applications. A game author would have to specifically request these features for them to impact game performance. In other words, it's turned off when you're gaming.

Steve: Yes.

Leo: So you don't need it.

Steve: Well, it's turned off anytime and always when it's not specifically needed for creating protection from the media to your eyeballs. And so we can assume that this won't affect gaming. What we don't know, and this may be patches and service packs away, is whether Vista is going to be a smooth and powerful gaming platform. Again, there are anecdotal reports saying that Vista is not nearly as good at this today as XP has been. But again, it's not even released yet.

Leo: We don't know. Actually, as we do this podcast, it has not been released. By the time you hear this it will have been out for a couple of days. It's going to be a month or two before really we know. And some of this might have more to do with DirectX 9 and 10 than any – this is a whole new platform. DirectX 10 changes everything. So it's hard to know what to blame if things are slower or not as reliable.

Steve: Well, I'm glad we did this, Leo. I'm glad we ran through these questions because there were some points that David brought up that I think did clarify some things that were big concerns from what Peter brought up. And it does sound like Microsoft is feeling painted into a corner by this. And I think it's unfair because they had the choice of allowing Vista to be a DRM content delivery platform or not. On the other hand, this does make me less excited about moving to it than I would have been otherwise, although I wasn't moving to it anyway.

Leo: Yeah. He's reassured us on a number of things, that copy protection won't affect the whole system, just the hi-def content playback. And I think that in many ways this is reassuring. And frankly, you always have the feeling when we're talking about this stuff that we might be kind of overreacting. It's just it's hard to say what it's going to mean until

it actually comes out and people are using it.

Steve: Well, and if in fact he's right about there being quality restriction and Macrovision protection and other things already in XP, it's worth noting that XP doesn't seem to be giving anyone a lot of trouble. Certainly, though, it's not the case that XP has anything like this massive redesign which has been perpetrated for the purpose of allowing AACS essentially policy to be pushed through all the way to the end user.

Leo: Right, right. We'll just have to wait and see. We'll find out. It's certainly a worthwhile discussion. It's fascinating discussion, and you can imagine over the last two or three years that there's been a lot of talk back and forth between Microsoft and Hollywood and vendors, these IHVs. This is not an easy thing to implement.

Steve, it's not an easy thing to explain, you do a great job. I thank you so much. We thank our sponsors, the Astaro Security Gateway folks, for providing us with support to make the wherewithal to make this podcast a reality. We couldn't do it without them. If you are looking for superior protection from spam, from viruses, from hackers, complete VPN capabilities, intrusion protection, content filtering, an industrial-strength firewall, and now new encryption capabilities as well, all in a single, easy-to-use, high-performance appliance, you need the Astaro Security Gateway. I've got a 120 right here, and I just love it. It's great for small or medium business. Call Astaro for a free trial in your business of the Astaro Security Gateway appliance. It's Astaro.com, or call 877-4AS-TARO. And if you're noncommercial, if you're non-business, you can download this software. It's open source. Use it. You can even – I think it's something like 79 euros a year – subscribe to the other features and get all the benefits. It's just a remarkable product. Astaro.com. Thanks so much for supporting Security Now!.

You could find more about this, including a transcript, both of Dave's questions and answers and of Steve's responses, on Steve's website, GRC.com. Elaine does transcripts for us. We have 16KB versions for those of you who don't want to download the big file, and comments, and that's where you can ask questions of Steve for our Q&A segments. And of course where you can find ShieldsUP, SecurAble, Shoot The Messenger, DCOMbobulator, and all of his great security programs, and the best disk recovery and maintenance utility ever written, ever will be written, SpinRite. Read some great testimonials at SpinRite.info. You have very – you are beloved by your customers. That must be a nice feeling.

Steve: Well, I think what I like about it is that anyone who's publishing software is saying, hey, you know, ours is the best this or the best that. And there's nothing better, I think, and more true and persuasive, than actual users reporting how they were able to use the product. And so in our case, in SpinRite's case, since it's not just giving them larger fonts or changing the clarity of their resolution or whatever, it's really coming to their rescue and aid all the time, it makes for some really great reading.

Leo: It's just great. I am so glad that you wrote SpinRite. I've used it, and it's saved my bacon many times. And I hope others will check it out at GRC.com. We're going to be back next week for yet another thrilling, gripping edition. We're actually going to talk about Data Execution Prevention next week.

Steve: Right. I still believe, I continue to believe there is probably no single more important thing people could use than preventing buffer overflows. We're talking about all the time; the security industry is talking about it all the time. This is the way remote hackers are able to send

something into someone's computer and essentially find a vulnerability to exploit and run their own code. With Service Pack 2 of XP and ever since, and of course in Vista as well, there is this data execution prevention support which requires hardware to be able in order to essentially turn this on. The reason I wrote SecurAble was to let people know if they had DEP support in their hardware, as anyone who's purchased a processor for about the last two years will, although unfortunately Microsoft has it defaulted to "off" in most cases.

Leo: Forward compatibility, of course.

Steve: Exactly, for backward compatibility. So they don't want to suddenly have Windows not working. But unfortunately what it really means is that Windows is much less secure than it could be. Next week we're going to talk about that some more and go over it in a little more detail.

Leo: Great, that should be fun. We'll see you next week. I'm Leo Laporte for Steve Gibson. Thanks for joining us. We'll be back next Thursday for another Security Now!.