Vista DRM Wrap-Up and Announcing "SecurAble"

Description: Following last week's guest appearance by Peter Gutmann, Steve and Leo wrap up the topic of Vista's new, deep, and pervasive Digital Rights Management (DRM) system. Steve also announces the completion and availability of his latest freeware: "SecurAble."

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-075.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-075-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 75 for January 18, 2007: Vista DRM.

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

Steve Gibson, laboring away at his lab of security at GRC.com, has come up with...

Steve Gibson: My fortress of solitude.

Leo: Your fortress of solitude has come up with yet another great application, SecurAble. We're going to talk about that because it's time, it's time. But before we get to that, Steve, I don't know, I hope a lot of people heard last week's episode. And if you didn't, I almost want to say pause the iPod and go back to 73 because...

Steve: Oh, Leo, don't almost say. Absolutely say it. Because I do want to continue on the topic a little bit more. I was sort of – I really wanted to give Peter a chance to explain things, and I really think he did. There were some points that I was sort of trying to slip in that I want to make sure got made because there is so much hysteria now. Even mainstream articles that I'm seeing are wrong about what they're saying Vista DRM is. So absolutely, let's assume that anyone listening to this has listened to last week's interview with Peter because it was really fantastic.

Leo: I think he made such a good case. I've read various critiques on the web and stuff.

And in general I think they've completely missed his point. And just to recap, I think one of the most significant points is, well, you could say Hollywood required this, but nobody made Microsoft build this into all versions of Vista. And in the last analysis, that doesn't seem like a very good decision. I think Linux, and I hope Apple, will say this should be separate. This should be in a box. And I think that's why Apple did this Apple TV. It should be external to the computer. You shouldn't hobble everyone with this premium content copy protection.

Steve: And you might suggest, for example, that there would be a Vista Media Center Edition in the same way that we had that with XP. The reason it's not feasible is that this stuff is literally down in the kernel. It required so much change to Vista that they weren't practically able to do a Vista DRM. And actually that sort of brings up another point, too, is that as I've been reading again, I feel like for the fifth time, the Microsoft specs...

Leo: I'm sure it takes five readings, to be honest with you. This stuff's complicated.

Steve: And there's a lot of interaction among these components. But it's another issue that's more clear to me now is that what they've done is basically created a heavily DRM'd OS, that is, it's not just for protecting HD. It may have been driven by their interest in doing that. But they make a point in some of their papers that there's been a lot of DRM that's had to be installed by third parties on prior versions of Windows because Windows didn't itself have a deep enough native digital content management system to satisfy everyone. Well, that's really been fixed in Vista. So they didn't want to just have, for example, a media-laden version that had all this stuff. They really want Vista to be a digital rights management platform that other non-Hollywood, non-AACS HiDef video content users can now rely on for protecting whatever it is that they want to put DRM on. So it brings all that along, too.

Leo: One of the things I guess we wanted to do in this episode is kind of circle back and talk about some of the things that we either didn't raise in 73 or maybe weren't completely clear.

Steve: Exactly. And I have actually got in my head...

Leo: Before we do that, can I just get the commercial out?

Steve: Oh, yeah, please.

Leo: All right. I hate to tease people. But I really do want to mention that Astaro is supporting this podcast because they've been so great. They're back again this year, and they are a wonderful product which we can really stand behind. That's kind of the reason that we were so glad to get them back for 2007.

Steve: And they're supporting Security Now!.

Leo: Yeah, exactly. Steve asked me before we went on the air, now, we're going to keep doing this for a while? I said, hey, as long as Astaro keeps paying for it, absolutely. This

right now is the only TWiT podcast with a sponsor. And that makes you golden, Steve. So we thank Astaro, makes of the Astaro Security Gateway. I have one, and I am blown away by it. It's great quality. I mean, the thing is rock solid. If you're a small or medium business, and your network needs superior protection from spam, I mean, listen to what it does. This is one box. Looks like a router; about the size of a router. But it's so much more. It does antispam, antivirus, content filtering. Of course it's an industrial-strength firewall, so it protects against hackers. It has intrusion detection built in. It's a complete VPN server. That's what I've been using it for, which is fantastic. I mean, I use all of the features. And it's all in one easy-to-use, high-performance appliance. Now, you can try it absolutely free in your business. Visit Astaro.com or call 877-4AS-TARO. Make sure if you do that that you mention that you heard it on Security Now!. And by the way, I also want to recommend it for noncommercial users. You can download the software for free. If you decide you like it, you can get all those additional subscription features like antispam and content filtering for a very low yearly cost, much less than you're probably paying for the software versions of these programs. Astaro.com, and we thank them for their support.

All right, I'm sorry, I didn't mean to interrupt there. I just wanted to get that done. Let's get back...

Steve: No problem. Okay. I'm holding the "Output Content Protection and Windows Vista" document written by Microsoft in my hand. And before the show I went through, during my fifth reading of this thing, and just highlighted some sections that I want to read verbatim so that it's sort of like on the record, and we can talk about these things. For example, in the introduction Microsoft says, and I'm just reading from their document, "We are working actively to ensure that a Windows Vista PC supports the needs of both consumers and content owners, and that it works seamlessly across a broad range of other devices, networks, and protocols. As we move towards the next evolution in the distribution and consumption of content, we are working on many fronts to create new experiences that drive the industry forward. This requires the ability to respect business rules across many dimensions, including content coming into a PC from cable, satellite, over the Internet, or on a physical media such as next-generation DVDs; management of the content on the PC, including providing a robust infrastructure that allows ISVs to add value without needing to worry about supporting DRM natively in their own applications; and respecting business rules as content leaves the PC. This paper talks about one aspect of the content protection work. It addresses increasing the security associated with video and audio rendering on the Windows Vista PC platform."

Leo: That's the key is video and audio rendering. It doesn't impact other stuff generally.

Steve: Actually it does. And in some...

Leo: I'm trying to put a good light on this sucker.

Steve: I know. Well, no, but in some good ways. One of the things that I've been distressed about over the last two weeks and our two episodes is that many people are swearing off Vista. They're saying, oh, I'm never going to go to that thing because I don't want to be burdened with all this. I don't want all of the scary things that Peter was talking about to be in the machine I own. I'm distressed because, as we have said in looking at Vista security previous to this, there are many good things that Vista is doing. I mean, Paul Thurrott has become a fan of Vista by using it. I'm running it on one of my tablet PCs. And in fact, in last week's episode you were asking Paul about Vista on a tablet. They're done beautiful things. And it's going to be installed on all the machines that people are buying next month. So it's clearly going to happen. So I'm distressed by the fact that there is no way around the fact that Vista is also a

pervasive digital rights management platform. I mean, we're getting a lot of good from a security standpoint, and the content providers are getting a lot of good for their own security.

Leo: Yeah.

Steve: Which sometimes, exactly, which sometimes runs against the freedom and flexibility that even honest users of content would like to have. I appreciate the fact that I can buy DVDs, and I can recompress the content and watch them on my PDA while I'm flying around the country. It's really useful to be able to do those things.

Leo: I'm willing to give that up. I just think that the content protection should be stuck in a DVD player or an external box in some way outside the computer so that we can still have our general-purpose flexible computers. The real problem is that the content industry sees any personal computer as a threat because any personal computer can be used to crack stuff. And they would like to make sure that all personal computers of any stripe, including Linux computers, have this kind of protection in it, to protect them.

Steve: Well, speaking of which, I received last week the second-generation Toshiba HD-DVD player. That's the HDA2, which is their – it's the standard...

Leo: I had that on order until LG announced the dual format. So I'm waiting to see what the dual format – because then I'm thinking, well, maybe I should buy – although I like HD-DVD. But maybe I should just buy that dual format.

Steve: Well, and if Apple's going to go Blu-ray, there's another strong driver of the Blu-ray format.

Leo: Apple and HP will. But so you got this new standalone player.

Steve: And just out of curiosity – I mean, this thing is phenomenal. It's got network configuration in it because there's an Ethernet connection, and you configure it for DHCP or give it a fixed IP, just like a PC, which is for it to enable it to update its firmware in case bugs are found in it or things need to be changed. So I was curious about what's in this thing. So I flipped to the back of the manual, under the license information, and get a load of the things that are covered by the license: Linux kernel, busybox, glibc, openssl, and...

Leo: It's all open source software.

Steve: Yes. It is completely built on Linux and open source software.

Leo: I'm not surprised. My Panasonic TV also has the GPL in the back of the manual because it's got Linux and openssl and openssh in it. That's so funny.

Steve: So they've used a lot of open source software, but of course there are...

Leo: But that's fine. Hack open source software and put it in your box. Just don't modify my Linux, that's all I care about. I think you made a really good point last week that the success and the strength and the power of the personal computer platform has always been because it is an open platform, and you can do things like that.

Steve: Yes. And get a load of this. Again reading from Microsoft's document, they even say that. They say, "A consumer electronics device is a closed box. Users can't load software onto it or add cards to capture content. At least that is the current perception of premium content providers, though it might not be true for future CE devices. By contrast, the Windows-based PC is designed to be an open platform. Anyone can load software on it." Unfortunately, malware authors can, too. "It is easy to write..." That's not in the Microsoft document, by the way.

Leo: Didn't think so. That sounded pretty parenthetical.

Steve: Sorry about that. "Anyone can load software on it. It is easy to write software for it because all the interfaces are well defined and published. And there are many good software tools available. The PC buses are also well defined, and anyone can design cards to plug into these buses." Continuing to read from the document: "The openness of the hardware platform is essential to a vibrant PC ecosystem. In the current world, however, the industry is also working to prevent hackers from using that openness to pirate copyrighted content. The goal is to make the Windows-based PC a safer place for premium content, so that content providers will be happy to allow Windows-based PCs to play their content. The term 'premium content' is used in this paper to refer to valuable content that needs to be protected from stealing. Each content type has its own particular policy that defines what the user can and cannot do with it. The term 'high-level premium content' is used to refer to the most valuable content types, such as high-definition DVD and Blu-ray DVD. The content industry may introduce robustness rules and testing that would effectively lock out PCs from premium content by not allowing PCs a license key for the encryption system used by conditional access systems or HD-DVD and Blu-ray DVD. These protection schemes will be very strong..." – huh, baby. It doesn't say that, either – "...in the future..."

Leo: I wish it did, though, don't you? Oh, baby.

Steve: "...based on AES, Advanced Encryption Standard, RSA, and so on. Under these future rules, a PC would only be granted a license to play the content if it is at least as secure as a consumer electronics appliance. To make the PC safer for premium content, Microsoft..."

Leo: Safer.

Steve: Safer, I know, "...has been working with members of the PC industry to solve the technical issues in hardware and software. Our key partners in this work have been Intel, ATI, NVIDIA, S3, and Matrox. While preserving the general openness..." – ugh. Doesn't say that, either – "...of the PC hardware platform, new solutions must be able to resist attacks against protected content. These solutions must also preserve the Windows experience for legitimate users, particularly without jeopardizing their privacy." So that's sort of their...

Leo: That sounds very good, but...

Steve: It does.

Leo: But really I have to say I don't know if that goal is possible. To me, the question comes down to what is your personal computer, an open platform or a consumer electronics device?

Steve: Well, exactly. And so then this starts getting more specific. There's an acronym soup, of course, once again. They have something called PVP-OPM. PVP stands for the Protected Video Path. OPM stands for Output Protection Management. And Microsoft's document says, "Typically, PVP-OPM operates within the Windows Vista protected environment and enjoys the software protection this provides. The protected environment checks for any unsafe situations for high-level premium content and turns off playing the content if an unsafe condition is found." It says, "To work with PVP-OPM, a graphics card manufacturer must provide for the following: 1. Output protection management capability on all board outputs. At a minimum, provide the ability to turn off every output. 2. Device driver capability to report reliably about the board outputs and their settings. 3. HDCP..." which we know is HiDef Content Protection. Or no – yeah. These acronyms are amazing.

Leo: I know. It's amazing you can keep them straight.

Steve: "...for DVI and HDMI outputs and Macrovision and CGMS-A protection on analog TV outputs. Otherwise outputs will be turned off by the PVP-OPM software. And finally, the ability to pass video through a constrictor, that is, a downscaler followed by an upscaler, so that the information content of premium video can be reduced when an unprotected output such as analog VGA is present."

So these are the things that Peter was referring to. But to do this requires closing down to a great degree the previously open architecture. It says, "The graphics hardware manufacturer must do whatever is appropriate to prove that the driver is talking to genuine hardware. If a particular implementation proves to be insufficient, as highlighted by a hack or a valid complaint from content owners..." So now content owners are able to complain.

Leo: They get to say, yeah.

Steve: Get this. This is Microsoft's document, "...then the related driver might need to be revoked."

Leo: That's the thing that bugs me.

Steve: Yes.

Leo: Go ahead.

Steve: "And a new driver would have to be deployed with additional HFS tests."

Leo: So all of a sudden your computer could stop working.

Steve: Yes, yes.

Leo: Your video driver could be revoked.

Steve: And they clearly...

Leo: And as Peter pointed out, that could happen just because they stopped paying their fee.

Steve: Yes.

Leo: It's not merely, you know, if the company went out of business it could be revoked.

Steve: Right. Here in the document, under this HFS and drivers supporting multiple chips, they talk about the risk of a single driver supporting multiple chips because, if that driver were revoked, it could affect much more than a single chip vulnerability. And literally, again, reading from the document, it says, "The Windows Vista protected environment will, after due process, revoke any driver that is found to be leaking premium content, either itself or from the hardware it controls. If the same driver is used for all the manufacturer's chip designs, then a revocation could cause all of that company's products to need a new driver."

Leo: Peter pointed that out in his article, that these unified drivers are going to disappear. It was nice. You could go to NVIDIA, download one file, it would work on any NVIDIA card. But that's not going to happen anymore.

Steve: Right. And that, of course, does substantially increase the cost, which ultimately gets passed on to the end user, which is of course the real reason that he was talking about the cost of Vista DRM. On this issue of tilt bits, Microsoft's document reads, "Tilt bits are provided in the DDI..." – that's the Device Driver Interface – "...as the driver's mechanism for reporting that a hacker is suspected. If at any time the graphics driver determines that something improper has happened, then it can set the appropriate tilt bit, for example, if the hash of an output status message doesn't match the message. If any tilt bit gets set, then Windows Vista will initiate a full reset of the graphics subsystem so everything will restart, including reauthentication. The tilt bits are also used by the driver in the PVP-UAB." That's another one of these acronyms. UAB is the User Accessible Bus. That is to say, if you had a separate graphics card, rather than integrated graphics on the motherboard, where Vista goes really, well, I can't say go overboard, but Vista's very concerned about any non-encrypted, I mean, the whole idea is not to allow any exposed non-encrypted content anywhere, literally from soup to nuts, from original content all the way to your eyeball. I mean, if they could encrypt somehow the...

Leo: They'd love to put an HDMI port in your brain.

Steve: Exactly.

Leo: With HDCP in there, too.

Steve: Because they're worried about someone literally using a digital video camera against the screen.

Leo: We'll talk about that in the 2021 edition of Security Now!.

Steve: So they say, "There is no requirement regarding the circumstances under which a driver should set a tilt bit. Adopting this mechanism is another example of the hardware manufacturer showing their intent to properly protect premium content."

Leo: That was another thing that he talked about is this notion of intent, yeah. That's really what they want you to do. It's not merely that you've – in fact, the spec isn't that clearly written. They just want to have you prove that you care.

Steve: Well, and it really sounds like, as I've read this again and again and again, it sounds like they're trying, Microsoft is trying to help to prevent lawsuits against content leakers. And so the more intent a hardware provider demonstrates, the better their case will be against the industry that brings a suit against them for allowing their subsystem of Windows to leak content. And that's where this showing intent is coming from. Because it actually says in this document, it talks about not doing a sufficient job and the kinds of onus that the hardware maker or software driver author could be subjected to. And then under this issue of resolution constriction Microsoft's document says, "In the future, some types of premium content, through its content policy, will specify that a full-resolution analog VGA output is not allowed..."

Leo: Oh, boy.

Steve: Uh-huh, "...and that the resolution must be reduced. It is not practical to change the actual scanning rate of the display, particularly because some displays are fixed resolution. But what is important is that the information content of the signal is reduced to the resolution specified by the content owner."

Leo: I just want to shoot them now. I just – that's just infuriating.

Steve: And here's the line. "Basically, a high-resolution picture needs to be degraded to make it soft and fuzzy."

Leo: Now, that's just for premium content, although it sounds like, if they're saying it has to happen over the VGA, does that mean if it's just my Windows desktop it's soft and fuzzy?

Steve: Well, okay now. Let me see if I was through here because there was a great point that you're making. Oh, there's one more thing here.

Leo: Keep going. We'll get back to that.

Steve: Okay. This is under content industry agreement hardware robustness rules. And this just, again, for anyone who's used to the open platform paradigm that created the PC, this

reads, "Content industry agreement robustness rules refer to, among other things, how a hardware manufacturer lays out and generally implements circuit boards. The rules are determined by the content industry in discussion with implementers and are described in, for example, the 5C, DTCP, and AACS documents, which are referred to in this paper as 'content industry agreement documents.'"

Leo: Yeah, that's the problem. Not an engineer. A bunch of lawyers who know nothing.

Steve: "The intent of the hardware robustness rules is to make it very difficult for hackers to use the graphics card or motherboard to extract video data. Interpretation is required..." – I love this – "Interpretation is required for some of these documents, and it is sometimes difficult to determine conclusively what is allowed."

Leo: Interpretation. Simultaneous translation. For crying out loud. It's a foreign language. Even they admit that.

Steve: Yes. Microsoft says, "Content industry agreement hardware robustness rules must be interpreted by the graphics hardware manufacturer. Vendors should work to ensure that their implementation will not be revoked for playback of high-level premium content as the result of a valid complaint from the content owners.

Leo: So we can't tell you what they might complain about, but you'd just better be sure you don't get a complaint.

Steve: And finally, "If it is found, for example, reported by Hollywood, that a graphics chip manufacturer is allowing 'hacker friendly' cards to be manufactured with their chips, and if that chip manufacturer is unwilling or unable to stop those cards being manufactured, then the final recourse would be the revocation of the driver for that chip.

Leo: I want to make this clear. That means they can reach into a Vista PC remotely and make that video card stop working.

Steve: Yes.

Leo: I mean, it's not like from now on all cards sold. That means my system right now – how would they revoke that? Is it done in Windows Update?

Steve: Oh, absolutely. It would be done through Vista updating its license keys.

Leo: Which it has to do or you can't use it.

Steve: Well, that's exactly right. The graphics card manufacturers have keys, and they are entirely revocable basically at anyone's whim. Anyone who's able to demonstrate that the card is leaking content would – now, hopefully it could be fixed in the driver. So the idea would be Windows Update would update your driver; and again, driver updating is then no longer something you could voluntarily choose to do or not do. You would update your driver or suffer

revocation, the idea being that it would update the driver, the driver would have new keys, and the old keys would then be revoked so no one who did not update their driver would then be able to play the content. The idea being the industry wants to retroactively be able to go out and fix any mistakes in software or hardware. The problem, of course, is that model says we could fix it in software. If in fact a highly popular card were found to be hackable, so that content could get out of it, digital content could be recorded from it, then at the discretion of the content providers they could require that that card, that is to say all cards of that hardware, no longer be able to play premium content.

Leo: Oh, the card would still work on the computer, I just couldn't play a DVD back.

Steve: Correct.

Leo: Oh, okay. I was a little scared. I thought the card driver would stop working in its entirety.

Steve: No. And that brings us that to that point that I referred to as an important segue just before we started talking about this last bit. And that is, it is extremely important to recognize that all of this is controlled by content policy that is bound to, cryptographically signed, to the digitally protected content. So it is a function of what the provider chooses to do. So the idea is that...

Leo: The idea is you're screwed, is what the idea is. I'm really – but I do want to underscore that because I think I misunderstood it. It sounded like the whole thing would stop working. I'll still be able to use my PC in every normal respect. But I just won't be able to watch a HiDef DVD.

Steve: Yes. And the point I was...

Leo: Are we sure that's true?

Steve: Yes, we're absolutely sure. And in fact...

Leo: I'm a little less perturbed, then. Because I'm never going to put an HD-DVD in my computer. I'm going to watch it on my TV.

Steve: And it's why I wanted to make this point, why it was so important to make this point, is that even today, as far as we know, current versions of HD-DVDs are allowing full resolution output from component video.

Leo: They haven't yet kind of enabled this bit.

Steve: Well, yes. The policy that is bound to the digital content is not saying disable component. Now, for example, my HD-DVD player, this brand new Toshiba that I got last week, it's got HDMI digital output and component video. And component video has been around for years. Many consumer devices, home theater projectors and so forth, have component video

and may not have the newer digital interface. So you can imagine that it would be very distressing for somebody who purchased this brand new Toshiba HD-DVD player and was watching HD-DVDs to find one that simply refused to play through their component outputs. So it's not clear that this is ever actually going to happen, which is one of the things I wanted to make clear. This is where so much of the confusion has come from. It is absolutely the case that it is possible for this to happen, but we don't know...

Leo: But the industry so far hasn't decided to do that.

Steve: Yes. And even revocation. You could argue that killing off hundreds of thousands of in-the-field...

Leo: Innocent bits.

Steve: ...working, yeah, video cards is really such a bad thing, you really have to wonder if the content-providing industry would choose to do so. They absolutely have the ability, but that doesn't mean they're going to.

Leo: Well, I don't blame them for wanting to preserve the right to do so, or kind of build it into the hardware. I just hate the fact that we're just kind of – they can hold that over our heads.

Steve: Yes.

Leo: So your point is, don't avoid Vista merely because of this. The security advantages are so great that you probably do want to go with Vista.

Steve: Yes. Well, okay. In laptops, for example, many people are buying laptops. There's an integrated system with on-card video. It seems to me laptops are more often to be something where you could imagine in the next generation watching movies than your Vista machine in front of where you're normally doing work. So a laptop could make a very useful content delivery platform. And it would be protected, it'll be running Vista, and you can watch HD-DVD videos on it probably without any problem. I really hope that all of this doesn't destabilize Vista, which was a really strong point that Peter made. We're hearing anecdotal reports all over the place that Vista seems flaky.

Leo: I talked to somebody yesterday who said it doesn't play videogames very well. He was trying to play DirectX 9 games, and they would frequently freeze or die. Now, we still don't know why that is. Could be a lot of reasons.

Steve: And there have been reports, again, anecdotal reports from people who are having problems with Vista currently playing movies of various sorts, depending upon what type of connectors they have. So...

Leo: I think HiDef content a lot of times will not play.

Steve: Now, I want to wrap up by talking about interfaces because the so-called last mile in Vista is from the output of the box to your display device. There are analog technologies which are not protectable, i.e., composite and S-video...

Leo: That's that analog hold that they were talking about.

Steve: Exactly. And even component video is an analog technology. Now, Vista will apparently add Macrovision and various types of copy protection to that, and compliant recorders will refuse to record that content if they see those protection measures have been stuck in. The two types of video interfaces are DVI and HDMI. Both of those are able to carry HDCP, the HiDef Content Protection, which basically allows the authentication of your display device itself back to the computer. So what I would urge people to do in the future is, if you are buying screens and displays that you want to be future proof, make sure they do provide HDCP, either with a DVI connector, a Digital Video Interface connector, or the HDMI.

Leo: But even farther than that, because we've seen some displays that have HDMI, but don't have HDCP.

Steve: That's true. And in fact...

Leo: And those you will not be able to play back HiDef content. In fact, that was part of the problem is that all of these "HDCP-capable" cards sold up to now are not.

Steve: Right. Well, because – and there are about nine things I wanted to say right there. Again, I don't think it's that it won't play it. But it won't play it crisp. It will deliberately run it through...

Leo: In some cases it will not play it, but it's supposed to downscale it.

Steve: It'll run through the constrictor. And again, the content provider in the policy that comes with the individual content is able on a...

Leo: So some disks are not enabled.

Steve: Correct.

Leo: Not all disks require this.

Steve: Well, and I've heard, again anecdotally, that no current HD content does actually do this.

Leo: Well, I'm not sure that's the case because I've heard, also anecdotally – and this is the problem, it's all anecdotal at this point. People have said, oh, gee, you know, I have a DVI connector to my monitor, or I have a component connector, and it won't play at all. So

it is possible that some disks are doing this, or maybe the hardware is doing it on its own recognizance without requests from the disk. I don't know.

Steve: Well, Leo, many people who have DVI – I'm completely DVI based. And not a single one of my computer monitors, which is DVI, has HDCP because they were never intended to be secure content delivery screens. They're computer screens.

Leo: So can you play HiDef DVDs on those screens?

Steve: No.

Leo: So you're saying that, even though the disk doesn't require it, the hardware is.

Steve: Correct.

Leo: So there you go. I mean, that's the problem is it's such an interlocking mess that there's all sorts of reasons why it might not work, all related to this content protection.

Steve: Right. And the other scary thing is that, again, what's happened is all aspects of this content delivery chain are now locked in licenses and proprietary intellectual property and revocable certifications. So, I mean, it is a new day. It is truly a big change. But again, I do wish that all Vistas were not laden with this technology because it does seem like it's going to make it twitchy. We really won't know for a while. But again, I'm sorry that there's been the scramble and the concern and the amount of FUD, essentially, that has come up because Vista does so many good things security-wise. I would not like to see people avoiding it. And you could argue, though, that the people who want the freedom of doing with their content what they will are probably the people who will stay on XP for the freedom and are less in need of the security things that random consumers who just aren't into computers and are not listening to this podcast are going to get. And so Vista's things help those people more.

Leo: Right, that's a good point, too. That's right. And those people probably are not going to stay away because in most cases they'll just be buying a new computer with Vista.

Steve: Right.

Leo: All right. Before we wrap up, do you want to make an announcement?

Steve: Well, I do want to announce that the first freeware, the first GRC freeware to result from the Security Now! podcast, I mean, this is a direct outgrowth of our work here, is available for download. It's called "SecurAble." You can find a link on the homepage, or it's just GRC.com/securable.

Leo: Oh, I like that.

Steve: I knew you would, Leo. I did that URL for you.

Leo: You're a good man.

Steve: It is a very cool app. It has been an eye-opener for many of the people over in our newsgroup who have been pounding on it and beta testing it for me and nailing out all my little typos in the text. The thing that is so cool about it is it will show people the security ability of their system. Many people, it turns out, have, for example, hardware DEP-capable systems, certainly any who have purchased machines in the last couple of years, but they probably don't know it. The outgrowth...

Leo: So you'll get an output that says you could turn on DEP if you wanted.

Steve: Well, yes. And in fact what's happened is, we've learned so much already about DEP. I am extremely excited about it. My next piece of freeware is going to be called DEPuty. We already had an outgrowth from this one because it is really the case, and I can't stress this enough, that hardware DEP, when enabled properly – which is never the case by default because it does create problems for people – hardware DEP when enabled properly is the single greatest solution for all forms of buffer overrun attacks that has ever been seen. I mean, most things that have happened in the last few years would have been stopped cold if hardware DEP had been enabled. I mean, it is a massively good thing for personal security. And the good news is it's in XP after Service Pack 2. So this is one thing, I think it's the single most important security measure that can be taken. And so certainly in the future we'll be spending some more time talking about what hardware DEP is. And it's very important to recognize also that software DEP isn't DEP at all. It's just virtually useless.

Leo: Turn it on and use SecurAble to find out. What else will SecurAble tell you?

Steve: It tells you whether your chip has 64-bit capability and also whether it's got the virtual machine extensions, either from Intel or AMD, which allow you to run much faster virtual machines. That is, the virtual machine extensions essentially make running VMs more practical because they are able to run literally at full speed by taking a whole – by essentially offloading a lot of the work that software was normally doing onto these virtual machine hardware technologies. So it's a very cool thing, too. And of course virtual machines are good for security, so thus that connection.

Leo: Speaking of virtual machines, I just wanted to mention I met with VMware at Macworld Expo last week, and their beta for Mac is out, and it's impressive as heck. And I said, "Well, how are you going to beat Parallels? They're a third the cost." They said, "Wait and see." The beta is free right now. There'll be another beta in I think they said around May, and then they should have it out about middle of the year.

Steve: Very cool. We'll certainly be looking at it.

Leo: GRC.com/securable to get your copy of SecurAble. And of course GRC.com is also the place to get the 16KB versions of this show for the bandwidth-impaired, and Elaine's great transcriptions if you'd like to read along with Steve. And of course, let's not forget, one of the reasons Steve can do this show and write the free software is his day job, which is the

great – and I'm really happy to be able to give you a plug because it's such a good program – SpinRite. You can go to SpinRite.info if you want to read any testimonials. You got any good letters these days from – I'm sure you have lots.

Steve: I do. I've got just a really short one that I really liked because his subject was "Best Program Ever..."

Leo: Okay, that's a good start.

Steve: ...and then six exclamation points. And he says, "I would just like to thank you for saving me hours of work with your SpinRite v6.0 program. I had a HD [hard disk] that I could not read sectors on, and it wouldn't even boot. I ran your program, and it booted first try. I was amazed. I wanted to post this on your website for others to read, but I couldn't get that newsgroup program to work correctly. But anyway, thanks again. I back this product 100 percent. I was absolutely amazed how well it worked on my totally inaccessible hard drive."

Leo: Isn't that nice.

Steve: So I do love to get those little success stories. Those are terrific.

Leo: GRC.com, SpinRite. It is really the ultimate disk maintenance and recovery tool, if you have hard drives. And nowadays we all have many hard drives, so it really is worthwhile. It's a good idea to run SpinRite on them. How often do you recommend, maybe every few months or...

Steve: Yeah, about every quarter, I would say, because it actually does preventive maintenance. I have another letter that I will get to here in a couple weeks where somebody talks about how he purchased SpinRite just to support the Security Now! podcast and all the work I do at GRC.

Leo: That's nice.

Steve: And he had it around when his system died. And as it happens he had it on a floppy. Well, the way you run SpinRite is you run it in Windows, and it produces bootable media. So you can either make a bootable CD or a bootable floppy, if you've got a system that still has a floppy, or even a bootable USB dongle. But the point is that, if you're going to do this, you really do need to have SpinRite already running, that is, already moved to a bootable media when your system dies. Otherwise you're not able to use your system in order to make the bootable media. At the same time, you know, we're real good about licensing, so you could certainly run it on somebody else's machine or on a different machine of yours in order to make the bootable media. But in this case the guy had already gone through that and had his bootable version of SpinRite ready to go, stuck it in his computer, and it fixed it for him.

Leo: Excellent. Maybe run off and do that right now. SpinRite.info, and of course GRC.com. Steve, we'll catch you next week.

Steve: Next week is a Q&A.

Leo: I was going to say, are we coming up on that?

Steve: Yes, we're on a Q&A. I would imagine we'll have lots of questions about Vista DRM. And we may still talk...

Leo: Wait a minute, that's episode 75. That's not mod 4, is it?

Steve: Agh, wait a minute.

Leo: No, we've got two weeks for that.

Steve: I show us on episode – maybe I miscounted. I thought that...

Leo: No, you're right.

Steve: Peter was 74.

Leo: You're right, this is 75. I'm sorry, I'm out of sync. This is – you're right, absolutely right.

Steve: Next week is 76. So I imagine we'll be fielding some questions from people and some experiences and have another really great episode of Security Now!.

Leo: Somebody asked me, "How do you get your questions submitted to Steve?" They've been sending them to me. There must be a better way.

Steve: Oh, absolutely. The way everyone does is they go to the Security Now! page, it's GRC.com/securitynow. And then just, after the page loads, hit End, or just scroll all the way down to the bottom. And there's a form that you can easily fill in to submit your questions, and they come right to me.

Leo: That's easy. All right. Hey, thanks, Steve Gibson. Once again, another great show. And really food for thought for anybody who's moving to Vista. But the bottom line is the security benefits of Vista outweigh these other concerns. However, it might be prudent to wait a little bit. I mean, it comes out January 29th. If you're buying a new machine, it'll probably come with Vista. But I've already upgraded to Vista, and I don't notice any issues yet. But I think if you were on the fence at all, hey, wait a few weeks. It's not going to kill you to wait a month.

Steve: Well, and if you were thinking maybe of making the Vista the heart of a next-generation home theater system, I would make sure that you're going to be able to make Vista happy.

Make sure that your projector has a digital connection, not an analog one, because that is subject to being shut down or fuzzified. So consider that. I know that, for example, Mark Thompson loves SageTV as his, like, TiVo replacement.

Leo: But forget HiDef content on that.

Steve: Well, exactly. So although he does use it, you would never be able to use protected content unless all of your video pathway was digital and supported secure encryption with certificates and so forth.

Leo: Or you download everything from BitTorrent.

Steve: There you go.

Leo: Take that, Hollywood. Unghhhh. I wonder how Elaine's going to transcribe the various grunts, groans, and moans that we've done in this show? I can't wait. How do you spell "unghhhh"?

Steve: I'm sure she'll manage, Leo.