Listener Feedback Q&A #15

Description: Steve and Leo discuss questions asked by listeners of their previous episodes. They tie up loose ends, explore a wide range of topics that are too small to fill their own episode, clarify any confusion from previous installments, and present real world "application notes" for any of the security technologies and issues they have previously discussed.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-076.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-076-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 76 for January 25, 2007: Your questions, Steve's answers, #15.

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

Time for Security Now!. My favorite security expert is here, actually one of my best buddies of all. Steve Gibson, I always enjoy talking to you every Thursday on Security Now!. And, you know, Steve's so dedicated. I have to leave town next week to go to New York to do "Regis & Kelly," and then go on another geek cruise. And most of the other podcasts are going to have to take a couple weeks off because I'm out of town. But Steve said no, we will not miss an episode. Steve, I bow my hat to you, or something like that.

Steve Gibson: We're doing three today, Leo.

Leo: Wow. We've got some good episodes ahead. Anyway, I was looking at a device that would allow me, in theory anyway, to do these shows anywhere, even if I had just kind of lousy Wi-Fi. And we're going to test this out because maybe, you know, my dream is someday to be on a boat doing this show. We'll see. Steve's never giving up. He's never not going to do his show.

Steve: I love it. And I get to catch up on our episode numbers as I listen to where TWiT and the other longstanding podcasts are, so...

Leo: The only ones you can't compete with are the daily one, the Giz Whiz, and the KFI show because that's been going for three years. And it's going to continue on, apparently, so you'll never catch up with that one. But this is Episode 76. That's a mod-4 episode. That means in our mod-4 speak we've got questions and answers, our 15th question-and-answer episode this week. But before we do questions and answers, let's talk about last week's show.

Steve: Well, yeah. I have some errata. It's sort of, in general, sort of different things. First of all, toward the end of last week's show we mentioned that I had finished SecurAble, which is GRC's latest freeware, to show you what security-related features your processor, your system's current processor, has. What's funny is, I was working on the web page when – and it still wasn't public – when I went over to TWiT to check something and saw that, because you were on the East Coast, three hours ahead of me, you had already pushed out the podcast. So...

Leo: Oh, I'm sorry.

Steve: No, it's okay. I mean, normally it's sort of later in the afternoon or in the early evening. But anyway, so I quickly got the page up. But a couple people commented that GRC.com/securable was not present when they were listening to the podcast. So I wanted to make sure that everyone knew that only was the case for – I don't know actually when the podcast went up. But anyway, as soon as I saw that it was up, I put a page up even though I wasn't really finished with it. Then I continued to work on it for a few more days. So GRC.com/securable, it's also linked to from our home page, just GRC.com. And people will be able to grab this little bit of freeware, I think it's about 108K, which you know, Leo, is big for me. It's because I signed everything. It's got a kernel mode device driver built into it. It also has a whole bunch of text and some graphics. So it's a little larger than my normal 23K exe, but you don't have to install it. You just download it and run it, and it tells you what you've got. And actually there's a lot of really fun information on the Securable page that I think people will find interesting, as well.

Leo: Excellent. Well, that's my fault, not your fault. And you know what I've decided to do – because it is inconsistent. In fact, sometimes I forget till, like, Friday to put the podcast out because it's just whenever I think of it. So what I'm going to do is shoot for a consistent time every Thursday. Would noon Pacific on Thursday work for you, if we just say that's our goal, to get the podcast pushed out then?

Steve: Whatever you want to do. I think maybe we should be having this conversation off the air because if we commit to noon, then suddenly, for whatever reason, one of us isn't available or something, it's like, agh.

Leo: It won't always be noon. I have some new software, and perhaps I'm relying on it a little much, but I have some new software that supposedly will publish these on a schedule. And so I'm going to try it for these next three because I will be kind of incommunicado. If they come out at noon...

Steve: That works for me.

Leo: ...Pacific on Thursday for the next three weeks, then that's the commitment. If not, we'll have to take it back to the drawing board and see. But in theory I can enter it into this software, and come noon on Thursday it'll push it out. We shall see.

Steve: One other thing I wanted to mention, since we were talking about AACS so much – and of course we had Peter Gutmann on a couple weeks ago, and the whole Vista content protection thing, which actually is going to be our topic next week because we're going to talk about Microsoft's formal blog response to Peter Gutmann's paper next week.

But I did want to mention that I just, as actually catalyzed by all of this, I purchased a Toshiba, the second-generation Toshiba HD-DVD player. And I remember that we were talking about how it's Linux-based and so forth, and that thankfully it takes less than a minute to recognize the DVD when you insert it. The first-generation player apparently was a little under-powered in terms of its processing power, so it took really a substantial length of time to go through all the decryption mumbo-jumbo that any hi-def content that is all scrambled is going to require. So I've been – I've watched a few things. I watched "Tomb Raider," as I was saying I was going to. And also the first two "Mission Impossibles." I have the three-boxed HD "Mission Impossible" set. And I have to say I was not that impressed with the visual look of HD.

But then last night I watched "Pitch Black," which was the first – it's a sci-fi with Vin Diesel where he crashes on, with a bunch of other people, on a weird planet in the middle of nowhere. And they're besieged with the planet's native and not-friendly flying things. Anyway, it was stunning. And so I realized that not all HD-DVD is created equal, and that – it's funny because I was talking to Mark Thompson about this. And I was bemoaning the fact that the DVDs were all saying they were 1080P, which technically means their resolution is 1920x1080, which is substantially greater, for example, than my screen, which is sort of first-generation HD, which is 1280x720. So I can do 720P, that is, 720 progressive, but not 1080. Mark's feeling is content isn't even digitized at the higher HD resolution. And frankly...

Leo: It's upscaled, yeah.

Steve: Yes. And so the idea being, people who go to some real extremes to go to 1920x1080 to get 1080P may be really disappointed.

Leo: I've read a number of columns lately that suggest exactly that. In fact, even say that, if you have a good upscaling 1080I display – and some of it does depend on the software, the DSP in the TV. But if you have a good display that can upscale, it's going to look almost identical to a 1080P source.

Steve: I'm not surprised. And so my experience has been – I just sort of wanted to share this with everyone because all the viewing experiences were in the same sitting, same distance from the screen, same lighting conditions. And so I was really able to do some, for me, my very first quiet analysis of is hi-def worth all of this hassle, essentially. And I have to say that, on a properly digitized movie, it can be phenomenally better. But so far only one movie out of four that I've watched has really been a discernible difference, which I really thought was interesting.

Leo: I also have an HD-DVD player. I use my Xbox 360. I've been very impressed with the ones I've seen so far. "King Kong" looks fantastic.

Steve: Which of course is boxed along with the 360 player.

Leo: That's right, that's why I saw that one. I have "Seabiscuit." That looks very good. What else have I watched? I've only watched a handful. There aren't that many HD-DVDs. And ironically, I haven't seen any of the ones that you just mentioned.

Steve: The one that I'm salivating over, not because of the content, but because...

Leo: See, I choose them for the content, not for the...

Steve: Well, "Aeon Flux" is...

Leo: Oh, dear, one of the worst movies ever made. But I guess, if you like "Tomb Raider," you're going to love that.

Steve: Well, okay. And it is apparently, I mean, the HD DVD reviews I've read have said it's the best-looking disk they have ever seen.

Leo: Okay, so that'll be worth looking at.

Steve: So I really am interested in getting into seeing what the HDness of this is all about.

Leo: Same thing happened when DVDs came out. In fact, I remember when CDs, audio CDs came out, they were very bad transcriptions. And then eventually people realized, hey, you can't just take the record, play it into a microphone, and put it on a CD. And the same thing happened with DVDs, and I expect the same will happen with HD-DVD. Especially as discerning viewers start to become aware of this, they're going to have to. I mean, you see every defect on HD-DVD.

Steve: Right. Well, in fact, and last night literally the pores on their skin was very visible.

Leo: You know, we're shooting "Call For Help" in HD now, speaking of pores on my skin. We actually will be using, believe it or not, airbrush makeup. We started using it in Toronto, and that's for HD.

Steve: Right, very cool.

Leo: They airbrush your face on.

Steve: For those listeners who are listening to TWiT and also Security Now! – and I imagine there is probably a lot of crossover. I also listen to TWiT. And you guys were talking a couple weeks ago about the idea of a dual-format HD and Blu-ray format player...

Leo: And it's out now, by the way.

Steve: ...that LG had announced.

Leo: You can get it now.

Steve: And I don't know whether you ever noticed the price.

Leo: $1200.

Steve: Exactly. And so it certainly is possible to get a dual format. And frankly I had believed, and this was just from having heard it anecdotally, that there would not be dual-format players because licensing restrictions legally prevented it. But it's very clear that at least that's not the case. So there is hope that we won't always be stuck in this which format do I need to – you know, like the old Betamax-VHS debacle.

Leo: We're praying. We'll see. But I do like HD-DVD, AACS or not. I have to say I think it's a good format.

Steve: Well, okay. So here I am, I already had the projector, so basically I had to run an HDMI digital cable because of all of the copy protection stuff that supports HDCP. But once done, the good news is the HD-DVDs are not more expensive than regular DVDs. So it's like, okay, why would I not buy those? Well, the only reason I would not buy them is if I really had some need to do something with the content other than just watch it.

Leo: You're right.

Steve: Because if, for example, I wanted to strip out all the annoying commercials or the menuing system, I have done that with some of the regular DVDs that I own. I'll reauthor them for my own use so that you put it in and it just plays the movie, rather than forcing you to sit there and watch their own previews on movies that are now no longer news because you've owned this disk for three years. It's like, you know, that's really annoying. And the other thing that's interesting is that technically it's now illegal for me to do that; but when I bought the disks with the intention and knowledge that I could decrypt them and reauthor them or compress them for watching on my Palm Pilot, it was not illegal because fair use in the law, in copyright law, was in effect. So you wonder, wait a minute, I bought them with the intent of being able to do whatever I wanted to with the content that I felt that I had purchased. And now along comes the DMCA that makes it illegal for me to do decryption. It's annoying.

And speaking of that, I don't know if you picked up the news that our friend muslix64 has not only cracked HD, but now Blu-ray.

Leo: And that's because it's still AACS. It makes sense; right?

Steve: Well, but what's interesting is he didn't even have a Blu-ray disk. Somebody who bought a Blu-ray disk was playing the Blu-ray movie in Windows using the PowerDVD player, or

I think it might have been WinDVD, in fact. That guy took a snapshot of the memory image of the process, that is, the WinDVD process, while it was playing the movie, presuming that if it was playing the movie...

Leo: It would have the key.

Steve: ...the key had to be in memory. And what muslix then did was – well, so this guy packaged up the memory image and a couple chunks of the encrypted content, which are just files, after all, on his Blu-ray disk, sent them to muslix64. Muslix64, first of all, his decryption, he's continued to work on this since we first talked about it around the turn of the year, around Christmastime was when this news came out that, quote, HD-DVD had been "cracked," which is not the case. But it is the case that it is possible to find the keys. So what muslix did was, he did a – and the reason I'm bringing this up is it's some fun true crypto technology that we've talked about in the past. He did a chosen plain text attack, meaning that the keys are 128 bits. So you cannot just try every possible key. That would be a brute-force attack where you start with all zeroes and then all zeroes and a one, all zeroes and a one zero, all zeroes and a one one, and you just go through every possibility. Well, a 128-bit key you cannot brute force in any reasonable amount of time, as we've discussed in the past. But you don't have to try every possible key. You just have to try every possible candidate key. And the candidate keys are the ones that were in memory, that is, you don't know, in the memory image, you don't...

Leo: So you don't know where the key is.

Steve: Yeah, but it doesn't matter because the memory image is much smaller than all the possible keys.

Leo: Right. So you just do a rolling slide through the memory.

Steve: Yes. And it works.

Leo: Oh, baby.

Steve: It completely works. So all you do is you take the first four bytes and assume that they're the decryption key, try to decrypt a piece of encrypted content. And you know what the beginning of the encrypted content looks like because it's a standard MPEG frame. So if that doesn't work, you take bytes two, three, four, and five. Then you take bytes three, four, five, and six. Then four, five, six, and seven. You just slide along through memory. And our PCs are all fast enough, in a very short time basically you've searched the image, the software image of this thing playing, for the key. You find it, and then you can decrypt all the content of the disk.

Leo: Let's put it this way. It's probably faster to do that than it is for the DVD player to decrypt the AACS, given the speed of your computer's processor.

Steve: Yes. And so here again I think we're going to be seeing these kinds of things now coming out from time to time about AACS. And what it really means is that software players are a huge vulnerability for this entire class of new encryption. If the software is decrypting and you have access to the software, then you can't protect it. And this is fundamentally what I keep saying, is the reason this can't ever work the way the content providers want it to is

something in the user's control, over which they have control, is displaying, one way or another, an unencrypted result. Which means all the information to do the decryption has to be right there in order for it to be delivered to the end user. So anyway...

Leo: Sure, yeah. That's the flaw. People often say – we might even have a question in our questions today. But they often say, well, wait a minute, you say you can never crack an encrypted email. How come you can crack a DVD? That's precisely the reason. The key has to exist somewhere. Very, very, amazing, just – I love that kind of stuff.

Steve: Isn't that a perfect hack? I mean, it's just a beautiful hack.

Leo: And obvious, obvious. Let's get to the questions, shall we? We've got a good dozen from our wonderful, intelligent, perspicacious listeners, starting with Kenneth Kan of Boston, Massachusetts, who writes: Your recent podcasts have been very inspiring. After testing my system using SecurAble – yeah, from GRC.com, absolutely free – I had made sure that I had hardware virtualization and hardware DEP enabled. However, it seems to be only available on the Windows platform. Many technologies discussed on the show and some that I've researched in Wikipedia are apparently Windows exclusive. For instance, I've never heard of my Mac OS X having this ability, to magically randomize its memory space every time it boots. Does this mean Windows is way more advanced and secure than its counterparts on UNIX and Mac?

Steve: Okay, it was an interesting question. First of all, it's worth noting that the Address Space Layout Randomization, ASLR, first appeared on and is most commonly known over on OpenBSD UNIX. So that notion of randomizing the location of things actually didn't come out on Windows first, it was in the UNIXes first. And there actually are some utilities for even bringing this to versions of Windows. Two weeks from now we're going to talk about specific attacks on the hardware DEP, on the Data Execution Prevention stuff. So I'm going to hold off a detailed discussion for then, for our podcast #78 in two weeks. But it is not the case that Windows invented this, nor that this stuff is only available under Windows. And certainly it's the kind of thing that will be quickly adopted by the open source community because they're able to move so fast.

Leo: It's a good idea. Yeah, I don't think it's in OS X. Now, you would think that, because OS X is running on Intel, that – I know hardware virtualization is available. Is hardware DEP also available?

Steve: Well, it's certainly available...

Leo: Or if you flip a bit.

Steve: Exactly. It's certainly available to the operating system. And it turns out that Sun's Solaris, running on RISC chips, has also always had this capability. So it has been around, it just hasn't been a mainstream technology that a lot of attention's been given to. And of course, because I believe it's so potent, I've done SecurAble, and I'll be doing DEPuty afterwards in order to really help to raise awareness of this.

Leo: Eric in Lansing, Michigan asks: When using XP SP2, would we be safe changing IE7's

security from your recommended high to the default medium high – that is, that's how it comes out of the box – if our computer has DEP configured properly? In other words, would DEP prevent unsafe scripting? Oh, good question.

Steve: Yeah, isn't it, great question. So first of all, to explain a little bit, what Eric is saying is that he knows that I believe surfing is just not safe with scripting enabled. So my recommendation is that you convert your security, your normal Internet Zone security if you're using IE, to highest security, which disables scripting, and then you selectively trust those domains that you have decided to trust, and you only allow those to run scripting, or to run scripting only when necessary as opposed to by default. So he's asking, if hardware DEP will prevent exploitation, does that make scripting completely safe? And unfortunately it does not because, even if hardware DEP were able to completely prevent any kind of buffer overrun attack – and that's a little bit of a gray area, it certainly is very strong in doing so – scripting is still unsafe. Because, for example, what the hackers have now found out, and we saw this with a WinZip attack through IE recently, a couple months ago, they're able to invoke any ActiveX control using IE and then talk to it. So there might well be controls that you don't want Internet Explorer to have access to which scripting enables. So, no, I would say you really don't want scripting, even if you knew that there would be no buffer overrun attacks on scriptable ActiveX controls. It's still not safe.

Leo: It's not just buffer overruns that are the problem.

Steve: Right, it's scripting. Scripting is a bad thing to allow websites to do to you.

Leo: Although I was using the NoScript extension in Firefox, and I have been since we talked about this last time. It's such a pain in the butt.

Steve: I know.

Leo: I finally just said, I'm taking my chances. I gave up. And so this is always the balance, isn't it, between convenience and security.

Steve: It really is. Now, of course, running in a virtual machine solves that problem, too. If you're willing to, like, browse in a VM and shut it down and not save the things that it does, that's really safe, too.

Leo: Moving along to Topher Slater of Portsmouth, VA. He asks: How will retail respond when the key for my video card or HD-DVD has been revoked, and I want to return it? He's talking about that revocation process where the Motion Picture Association could say, oh, that video card doesn't do what we want it to do, we're not going to allow it to play back HD-DVDs or other premium content. He said: Or what happens if I buy a DVD and it will not play on my player? I have to open it in order to find out if it will work. As of now, they won't take it back. Am I stuck with a $20 piece of plastic?

Steve: It's a really good question. I really have to believe that the threat of revocation is easily blown out of proportion. It's such a bad thing for players, commercial players, to have their licenses revoked that it's difficult for me to believe it would ever actually happen. So, I suppose, I mean, we know it's possible. We know the technology is there. We know that the

content providers unequivocally have the capability of doing that. But I just have to wonder how big a problem it really is. And I don't want to scare people by saying, oh my god, because it can happen, it will. It very well could never happen.

Leo: I think, now having heard all the arguments pro and con, it would be such a costly, public relations-wise, thing for them to do, there's no way that's going to happen.

Steve: It would be a disaster.

Leo: It'd be the end of the, not the movie industry, but of the MPAA for sure.

Steve: And to get back to Topher's question, he's asking would he be stuck with a worthless piece of plastic, meaning his DVD. Certainly not.

Leo: And that's up to the retailer.

Steve: Well, yes. Well, the DVD is still playable. You don't revoke the DVD. You revoke the player or the screen or something in the encryption channel.

Leo: Well, here's something that actually is a real issue. You can go out and buy an HD-DVD thinking you have an HD-DVD player, which you might, but you don't have the properly encrypted monitor. This happens all the time; right?

Steve: Yes, very good point.

Leo: Yeah. And you get a black monitor because your monitor either doesn't do HDMI or does HDMI but not HDCP. That has been happening to people. And I guess that's up to the retailer whether they'll take it back or not.

John Hutchinson of Clermont, Florida, is worried about LAN-based viral spreading. That doesn't sound good. He says, I have a few questions regarding Windows filesharing. I use Windows filesharing extensively inside my NAT router for things like backing up data between machines using an old command script I wrote years ago and for just moving files around between machines. John, I do exactly the same thing. I back up all the time over my network. Sometimes I map a drive. Me, too. Sometimes I just browse using My Network Places. It's very convenient. I tend to shy away from mapped drives. I suspect that might make it easier for malware or viruses, should it get one on a machine or on my LAN, to propagate. I suspect, however, this is not much of a deterrent as, if I can browse My Network Places, so can malware. Secondly, I have nightmares of someone visiting with a laptop and loaded with bad things, using my Wi-Fi to connect and having bad things propagate on my LAN that way. That does happen. That's why Zotob knocked out CNN about a year ago. So my question is, do you have any recommendations regarding how to make it harder for malware to spread to another machine on my network, without sacrificing the convenience that filesharing provides?

Steve: No.

Leo: Oh, come on. I do. The Zotob worm and all of these other worms aren't an issue if you turn on Windows Firewall on each system.

Steve: Well, exactly. I was being a little facetious because...

Leo: You were being facetious. See, I've been listening to you. I know the answer.

Steve: Well, although with Windows Firewall up, then you still have a problem of making those machines connect. That is to say, if you have mapped drives, malware can see mapped drives. So the only thing I can imagine...

Leo: A mapped drive just means that that network drive has a letter, it's drive Z or whatever, and so you can open it as if it were a regular drive.

Steve: Exactly. It's very easy for something to see it.

Leo: And so malware wouldn't have to look on the network, yeah. It would just say, oh, hey, there's something on the M drive.

Steve: Yes, it would have to do no work in that case. The only thing I could suggest would be that, if all of your machines are in the same workgroup and/or domain, with the same username and password, then you're able to create a mapping without giving any credentials. However, if you deliberately had different usernames and passwords on the different machines, then you do have to create some credential, you have to give it the log-on credentials of the target in order to create the mapping, and no malware would know how to do that. So again, it makes it less easy to do this kind of filesharing. You have to not leave static mappings up against the danger that something could get into your machine and spread. And so that means you've got to bring them up and tear them down when you're not using them. And it's exactly what we always run into, Leo, like what you were talking about, about not using NoScript under Firefox because it just – it's a pain to have to give sites permission. Similarly, it's a pain not to be able to use static mappings. But if you want the security of not having that liability, it's going to be a little bit of hassle.

Leo: You know, okay. I map, but...

Steve: It's a balancing act. It's a balancing act.

Leo: It is a balancing act. I map, and I'm not too worried.

Steve: I use file mapping myself all over my network. And I'm just very careful not to let anything bad get in.

Leo: I guess my attitude is, if there's something bad on your network, you're dead anyway. Doesn't matter if you've file mapped or not. And if somebody comes in and uses

my network, which does happen all the time, I think that's why it is important to have an individual firewall on each machine as opposed to the NAT router because they're inside a NAT router.

Steve: Yes, very good point.

Leo: David Gladstone, not far from Peter Gutmann, he lives in Auckland, New Zealand, has been doing some thinking about Vista DRM. David says: I've been listening to your discussions of Vista DRM and revocation of drivers. My understanding is that premium content is not necessarily only available on HD-DVD or Blu-ray media. If so, I was wondering if it would be possible for a suitably crafty hacker to create a "viral video," in both senses of the term, that contained revocation lists for a bunch of non-leaking drivers, thus neutering the Vista platform. Wow, this guy's thinking real hard. I am sure there must be some cryptographic safeguards to prevent this. Maybe this is a weak link? Is there a single private key that, if compromised, could bring down the whole pack of cards tumbling down? That's interesting.

Steve: It really is interesting.

Leo: So let me understand what he's suggesting. So somebody puts a video up on YouTube. The video has revocation lists in it. And but wrong, illegal revocations lists somehow. And while you watch that video it's basically disabling the functionality of your video card. Is that possible?

Steve: Well, what prevents that is that there is a single central revocation list authority which is this – I believe it's the 5C Authority, if that's the same as who runs AACS. But anyway, it is the AACS Authority that maintains the master copy of the revocation list. All of the AACS licensed players have only the public key that allows them to decrypt the master revocation list. Nobody but the AACS has the private key, which they use to encrypt the master revocation list. So it is not possible for someone to basically make up their own naughty revocation list and get any players that are operating correctly to decrypt it and believe it and apply it.

Leo: Makes sense.

Steve: So really this whole, you know, the jump that we've had in crypto has been hugely leveraged by the AACS system, using public key and symmetric key crypto in every way you could imagine so that they, I mean, they really have thought through all these scenarios and done everything that they can think of to prevent it from being abused.

Leo: The good old public key cryptography helps everybody. SN listeners Mr. and Mrs. Sven Thomas of Caronport, Saskatchewan have been wondering – I love reading these. I just love it. It feels like old-time radio, doesn't it? Mr. Answer Man, we have questions about the HDCP and Vista DRM in general as they pertain to hi-def home video and high-end hobbyist video content makers. While it's clear that HDCP affects only HD and premium HD content that is played back from a commercial HD-DVD or Blu-ray disk, what about those of us who use, for instance, Sony Camcorders, hi-def camcorders, and produce hi-def content for ourselves? Is Vista and our future hardware, including that inside the camera, going to cripple my personal HD content, just because it's not digitally signed? Or

will the camcorder apply a consumer-type key that will allow any content we create to be played back in hi-def? He's worried that all this hi-def content protection is going to impact his personal recordings.

Steve: Right. And it absolutely will not because his personal recordings will not be encrypted.

Leo: So just as Hollywood could make a DVD that you could copy, you get to make a DVD, even hi-def, that you can give to your friends and everything. It doesn't impact you at all. So it's not the fact that it's hi-def that's the issue.

Steve: Exactly. And in fact, the same has always been true of regular old standard definition DVDs. If you create your own DVD, for example, from your home movies, converting your home old 8mm movies over to DVD, if you have some service do that, they'll almost certainly be producing a non-encrypted DVD, which is then freely copyable. I mean, if it's not encrypted, in no way will anything prevent you from doing whatever it is you want to do with it.

Leo: Dee Smith of Leesburg, VA says: I really enjoy your podcast seminars with Leo. So does Leo, by the way. However, the more I hear about Vista and the diabolical plans for hardware digital rights management, the more I want to find an alternative. Every two years or so I build myself a new system. It's about time for a new one, and I'm anxious to avoid all the embedded complexities that Microsoft is forcing on the hardware guys. All I want is a Core 2 Duo system that will perform well and do justice to my new 24-inch Dell monitor. I have no interest in HD media players. If necessary, I'll also stay with XP Pro for as long as I can, if that's what it takes to avoid Big Brother Bill. Any suggestions?

Steve: Well, I would suggest doing exactly what I'm doing. I have just put together a big Core 2 Duo – actually, mine is a Core 2 Quad. I named it Quadmire. And I'm installing Windows XP Pro. That'll be my new platform. Because first of all, we know that I'm a Luddite in terms of staying, like, one major step behind. I'm still using Windows 2000 as my main workstation. And so I'll be moving to XP. For people who are really put off by Vista, who don't feel that they're getting any benefit from Vista above and beyond, well, enough benefit to tolerate this sense of losing control over the OS and so forth and so on, then, I mean, I would just say stay with XP.

My sense is Microsoft may have a much harder time killing off XP than they want to. They've been forced in the past to continue supporting OSes or OS versions that they really wanted to shut down support for, but they weren't able to because of strong demand, mostly from their enterprise customers. They're less concerned about individual end users. But the enterprise customers just said, no, we're not going to be ready yet to move up to the next platform. And Microsoft's been forced to continue support. So I would be very surprised if Microsoft's able to kill off XP, given that the only choice is people going to Vista who just don't want to.

Leo: I wonder if Microsoft would consider making kind of a stripped-down version of, let's not say Vista, but let's say of Windows, that is for people who don't want all of this extra stuff.

Steve: That's been discussed in our newsgroups, over in the newsgroups on GRC. The reason it can't be done is – which is unfortunate because that would be a tremendous solution. And in fact, maybe you were talking about it on TWiT because I feel like I've heard this...

Leo: I'll put it this way. They do make a stripped-down version for the China market of XP, for the international markets.

Steve: And of course we have the, quote, "Media Center Edition" of Windows XP that would sort of lead you to believe, well, how about, like, a really non-media-centric version of Vista. The reason they can't is that all of this AACS and the so-called protected video path and the protected audio path, they have hugely changed the fundamental kernel of Windows in order to embed this stuff really deeply into the OS. It's not something you can simply remove. It's really been a pervasive change to the architecture of the OS, making it a solid DRM platform.

Leo: And also from a political point of view, they don't want to do this because really what you're seeing here is Microsoft's response to Hollywood's assertion that all a PC is is a piracy device. And really Hollywood would like to see all PCs neutered, regardless of what you want to do with it. They see them, every single one, as a potential piracy device. They say, look what happened to DVDs. That's how people use their PCs. So what Hollywood would like is for not one PC to be sold without this kind of copy protection on it. That's their goal. And I think to some degree Microsoft's acquiescing by making Vista. And that's why this DRM is built in to every copy of Vista, regardless of whether the machine comes with a hi-def player or not.

Steve: Well, we're going to have, next week, when we run through Microsoft's blogged response, David Marsh's response, I think a lot of these issues get covered. It's going to be really interesting.

Leo: Oh, good. Oh, I can't wait. That's next week, good. Microsoft's response. I can't wait to hear it. Rich in Highlands, Scotland – and I'm not going to do the accent.

Steve: Thank you.

Leo: Well, maybe I will. No, okay. Wants to find a new free email service. He writes: I have a problem. On signing out of my Yahoo! mail account I was horrified to discover that at the bottom of the page it said, quote, "Notice: We collect personal information on this site," end quote. I also noticed that after signing in, the URL changes from HTTPS, the secure HTTP, just to plain old HTTP://. I thought it might be time for a change from Yahoo!. I heard you talk positively about Gmail several times. However, I just discovered you have to be invited. Can you suggest somewhere I could make an email account that won't take my info and will stay secure? This is a real issue because I use my Yahoo! mail for eBay, Amazon, et cetera, and I'm now really convinced I should switch.

Steve: And this is actually a question for you, Leo. I thought maybe you'd have a better sense than I do. I mean...

Leo: I do.

Steve: ...I know about Gmail. I really like it. I would be surprised, if this guy knows anyone who has sent him email who has a Gmail account, he could simply write to them and say, hey, could you invite me to Gmail? I think I've got a hundred invitations sitting here.

Leo: Oh, I'll send him an invitation, yeah.

Steve: Yeah, exactly.

Leo: I don't know that Google is any better than Yahoo! in this respect.

Steve: And of course it is frightening because we know that they're archiving everything forever. Which is sort of frightening.

Leo: And we know that their business is advertising, just as Yahoo!'s is. So this Yahoo! disclaimer may be not something to really be terrified about. Every website collects a certain amount of information, like your IP address, automatically. So this may be a lawyer saying we'd just better disclaim this. I don't know that Yahoo! is somehow trying to cross-reference your IP address with stuff you do online and so forth. But if they are, Google just as well might be. There are, however, web-based mail services that are aggressively private. Probably the most so is Hushmail, at Hushmail.com. Hushmail is remarkable. First of all, it's PGP. All your mail is secured. It's built in. It's automatic. They also are extremely privacy sensitive. And their business is not selling advertising, it's selling Hushmail. They do offer a free version, but they also offer some very advanced business solutions. So...

Steve: And there's also COTSE; right?

Leo: CO – I don't know that one. COTSE dot...

Steve: I think .com, .net, I'm not sure. I think it's also a very strong...

Leo: The ultimate way of protecting your privacy online. Oh, that's interesting. I have not seen that one. Full-service privacy website, your shield from the Internet. So it sounds like they do proxy stuff, as well.

Steve: I know that they have mail, so...

Leo: And another email service that is also aggressively – now, I like Hushmail because it has built-in PGP, so there's a lot to be said for that. But SpamCop.net is an antispam site that is also aggressively privacy focused. So another – and I actually have a SpamCop account, as well. If you want to avoid spam or report spam, SpamCop is very useful there, too. So I'm going to have to take a look at COTSE. That's interesting. But Hushmail, Phil Zimmermann worked with them for a while, the creator of PGP. I think they're a very good group. And they have a lot of interesting features. But, I mean, email is not private, as we know. The only way it could be private is if you encrypt it.

Steve: Exactly.

Leo: Someone referring to themselves as "Anonymous Sender" says: At work we have web

applications which require testing from outside our firewall. Currently we attempt to do this with an iMac running OS 9 and a 56K modem.

Steve: Isn't that great?

Leo: Not the best solution, he says. We're wondering if it would be possible to use The Onion Router from either a newer OS X machine or a machine running XP to access our site as if we were outside the firewall. Oh, I see.

Steve: Brilliant, it's brilliant.

Leo: I see. So their web applications running on their site, and they want to test them as if they're a customer. I get it.

Steve: Yes.

Leo: If I understood your description of TOR, it sounds like using it would give us the same view of our site as we would see from outside the firewall because our incoming connection traffic would be coming from outside. Is this right? Any pitfalls I've missed?

Steve: That's brilliant. I think it's a perfect idea and solution. Yeah, it ought to work great. I mean, what they've been doing is they have a dialup ISP somewhere. They've been using their 56K modem to dial into the ISP and then surfing back to themselves from outside. And yes, The Onion Router ought to work. And because with The Onion Router you're able to determine the complexity of the onion network, you could just tell it, we just want to use one. So you'd have very little latency and other problems associated with, like, really long, multi-hop onion routes. So that's a tremendous idea.

Leo: Microsoft does have some tools, I seem to remember, for doing this kind of thing. But that seems like an easier way. Free, certainly, yeah. Bob Sudduth of Dayton, Ohio – you were born in Dayton?

Steve: I was born in Dayton.

Leo: Wow. From your hometown. How long did you stay in Dayton?

Steve: I wasn't even conscious, I think.

Leo: There and gone.

Steve: Well, I guess I was barely conscious. My sister was born in Fairborn, and I'm two years older than she. So I guess – and I think my parents left shortly after she was born.

Leo: What were they, on the run?

Steve: So I was two-point-something years old while I was in Ohio, and I've never been back.

Leo: Then to Fairborn, and then to California. Extrapolating from your discussion on Vista and DRM, what's to keep companies from being extorted by hackers? For example, if you don't pay us X million dollars, we'll disable all your drivers everywhere.

Steve: Right. And that comes right back...

Leo: Same thing.

Steve: Yes, exactly. I put this in there because many people have worried about this and asked the question. So although we just read Bob's question, this is for everyone who asked. Same story, is nobody else will ever have, hopefully, or that would really be a problem, the private keys for the public key crypto system that the AACS guards as an absolute secret, so that there's no way for anyone to spoof any of this information anywhere along the chain of delivery from the AACS. It's really interesting, in fact, there's something we didn't talk about because it was sort of an unnecessary level of detail. But even the production of the HD or Blu-ray that is an AACS content, nobody knows anything more than they need to. The content provider is given some keys. The actual manufacturer is given a different set of keys. And then of course the rendering machine, the computer or driver display, they're given their own keys. And they have this all kind of fixed together in an interlocking way. But nobody has the ability to do anything wrong with the system because everything is protected from everything else. So, I mean, it's a beautifully engineered system. It's just a pain to have it.

Leo: It works. Listener Ed from Philadelphia wonders: What are the security benefits of surfing the 'Net under a user account rather than an administrative account? Boy, I run all the time under user accounts on all my machines. I remember having heard of it several times on Security Now!, he says, but would you remind me? And by the way, this is not just on Windows. This is on Mac, on any operating system. You don't have to always run as an administrator or root or super user. You could run as a normal user.

Steve: Right. And in fact, of course this was all created by UNIX machines originally, where the administrative account was called the "root" account. And then you would use, I mean, even servers would log in as non-root users, so if they were compromised they wouldn't be able to do really damaging things to the system. So to answer Ed's question, the idea is that when you're surfing as a user account, or that is to say a limited user or a non-admin account, essentially the programs you're using are running with your privileges, that is, your log-on privileges. If those are limited, then the program's actions on the OS are similarly limited. So, for example, it's not able to launch code running in the kernel because that's not a privilege that a limited user has. Only an administrative user is able to do that. So the point is that the programs you run, run with the same privileges that you do. And so they're limited just like you are from doing bad things to the system.

Leo: There are some drawbacks to doing this because some programs don't work well if you're not a super user, a root, or administrator. I think a lot of programs don't. I found it to be a little bit easier under Vista than it is – in fact, a lot easier than it is under XP. So

they've fixed that problem from an operating system level.

Steve: Yes. In fact, Vista – at one point we will talk in depth about UAC, the User Account Control, because all users of Vista see is this box that's popping up all the time, asking them for permission to do things. It turns out there's much more going on under the hood.

Leo: Ah, interesting.

Steve: Yeah. It's some very potent, powerful, and useful technology. So we'll certainly be doing an episode of Security Now! to explain exactly what is User Account Control.

Leo: Even if you run as administrator, you see that UAC box. If you're running as a limited user, however, you'll be asked for the administrative password, which I think is a little bit more secure, I really do.

Steve: I agree.

Leo: And that's kind of how Apple does it, as well. Even if you're running as an administrator, you have to give it the password to actually give it the root permissions to make the changes it needs. But nevertheless, on both Apple and Windows, I almost – except for XP, where it's just almost undoable. But on Vista and OS X I'm always running as a limited user, and it works great. In fact, my only regret is that in Vista it doesn't kind of require you to set up a limited user account. When you set up an account, it's automatically an administrative account.

Steve: Yeah, I think that's Microsoft again, recognizing that it would just be too hard to sell for most users. And so but what they've done is, and this is what we will be talking about in detail, is even an administrative account, there's like a lack of automation for the things that can happen. If anything tries to do things that modify the operating system, there'll be a dialogue that pops up. And this is not just a regular dialogue. There's all kinds of protection around that simple-looking UAC popup that you're clicking "Okay" on. So that if some malware got in your system and tried to make a modification behind your back, even as an administrator it would not be able to do so without your permission.

Leo: Jeff Smith of Alpena, Michigan, after listening to my KFI show, I guess, has a question. Uh-oh. I hope I didn't say something stupid. I learned about a very cool program thanks to Leo and his KFI podcast. It's called CrossLoop and can be found at CrossLoop.com. It's a simple remote desktop – oh, yeah, this is really cool – simple remote desktop-type application which has been very helpful for me, the family computer geek. It's amazingly simple to set up and use, even for the beginner computer user. However, since I'm a listener to your Security Now! podcast, I'm curious if there are any security risks to myself or others by using this program. It's a remote access program. Mind you, it has never given me any reason to suspect it. I'm just a cautious person when it comes to my computer security. And I'm confident that you could give this program a thorough look at how it works.

Steve: What it is, is it's sort of a cross between VNC and Hamachi. And in fact it uses VNC's open source, I think it's the code from the TightVNC version, the open source VNC. Then what

they've done is they've added cross-router penetration like Hamachi does, so that essentially you're able to give the app to another person. You have a copy. Instead of having this notion of separate client and server, which can be confusing, you've just got two different tabs. One of them is the host, and one is the guest or however. I mean, the idea is that it's for desktop sharing, very easy desktop sharing. Then you create a user account for yourself. And it uses a 12-digit number to sort of authenticate. So all of that's good.

The only downside, and this is true of any service which is going to do NAT router penetration for you, like Hamachi or like this CrossLoop, is you are inherently trusting that external third party not to mess with you, not to play any games. Because both users behind their routers are contacting that third-party server. That's the thing which is negotiating their subsequent direct point-to-point connection between them. And that's how the NAT penetration works, as we've discussed in the past.

So again, he has no reason to mistrust the CrossLoop guys. We have no reason to mistrust them. I mean, I talked to, as you remember, Alex Pankratov, the original author of Hamachi, and was very convinced that he was a good guy. But I like the idea of having complete control myself. And so I shy away a little bit from – just anyone should be aware that the involvement of a third party does give them the ability, if they wanted to, to play games. Which is not to say they ever would or are. But that's a factor.

Leo: We don't know who they are, and so we don't...

Steve: And again, it's a tradeoff that you make in, again, a typical security tradeoff. If I don't want the responsibility for needing to configure my NAT router to, for example, doing a static port mapping into the router in order to get to my computer from the outside, if I don't want that responsibility, then I'm going to trade that for some little bit of security, probably not enough to worry about.

Leo: Right, right. Steve, we've completed 12 questions and 12 answers. Unbelievable. And since this is our 15th episode, that means you've actually done 180.

Steve: And we've got many more. When I checked my mail I had 600 postings from people came down. So we won't be running out of questions anytime soon, Leo.

Leo: We're glad to get the questions. Can you tell people once again how you find the questions? I mean, where to submit one?

Steve: Right. We have a form at the bottom of the Security Now! page. So just go to GRC.com/securitynow. The page will come up, and just hit "End" on your keyboard, or scroll to the bottom. There's a form there. People can be anonymous if they choose; or, in fact, if they want to get their questions read on the air, they need to use their name and tell us where they are. Not that we want to force people to be non-anonymous, but we like to be able to say, hey, Jeff Smith of Alpena, Michigan asked the following question. It's just more personal and more fun for us. So send a question to me, and I'll get it, and perhaps we'll read it.

Leo: And while you're at GRC.com don't forget SecurAble, Steve's new free security application, along with dozens of other security applications, including the great ShieldsUP. GRC.com is the place to go. And, you know, the one thing that's not free on GRC is the thing that is the most valuable, the great SpinRite program, Steve's bread and butter for

the last decade or so. It is the ultimate disk recovery utility. And by the way – or just maintenance utility. I run it regularly on all my disks to catch problems before they happen. And if something happens to corrupt your disk, or bad sectors, SpinRite can almost always recover those bad sectors, recover that data, and get you back on your feet. It's really a great program.

Steve: Well, and we're here for people, too. I received an interesting note from someone over Christmas. The subject was "Redownload SpinRite from remote location." And he first wrote to our sales address, which Sue monitors even through the holidays. And actually this was on the 23rd, so not on Christmas Eve, but the day before. And he asked, he said, just wanted to say thanks so much. Oh, when he first wrote he said: I purchased SpinRite a while back. I'm at my mom's for Christmas, trying to troubleshoot what looks like a hard drive problem on her computer. My SpinRite and license info is at home. Is it possible for you to email me creds to download a copy to try to run on her hard drive? And then he says: I think I registered either under blah blah blah or blah blah blah, you know, his two email addresses that he had. If you could send information to either of those addresses, I would be able to get them from here. Many thanks, and have a wonderful holiday. So Sue got his mail, looked him up in our ecommerce system, which I wrote from scratch, and it has all these capabilities.

Leo: Of course you did.

Steve: So she found him, sent his transaction code, which he didn't have. And the transaction code allows any of our SpinRite owners to download SpinRite from anywhere they happen to be. So, for example, if he had it in his wallet, he could have used that in order to grab a copy.

Leo: Keep your code with you at all times.

Steve: Well, you just never know when your mom's computer's going to crash out.

Leo: That's right. In fact, I'll be fixing my mom's computer next week, so I'm bringing my code with me.

Steve: What was really cool was he then followed up that letter. And he said: Just wanted to say thanks so much. I got the ISO, burned a CD, ran SpinRite, and now Mom's PC seems to be running just fine. He said there had been a failure in a Windows component related to Windows Explorer. So after boot, things just pretty much stopped working. He said: After SpinRite, it's all good. She's thrilled to have her email and web back, so you provided her the best Christmas present this year.

Leo: See, that's really interesting. Hard drive failure, you know, these big hard drives now are so huge, and it can happen at any time. And that can give you all these weird symptoms that, you know, I answer all the time on the radio show.

Steve: It's funny, I was doing some research on Seagate's site because I'm setting my new system up with serial ATA drives. I was talking to Mark Thompson, who was commenting they've got so many systems, they've got hard drive problems all the time. And he said it's mostly the newer disks. When I was on Seagate's site, I was a little surprised by their reliability claim. This is the spec sheet. It was a 7200.9, a Barracuda, brand new Barracuda SATA 7200.9

drive. They were saying they had 0.34 percent failure per year. I'm going, wait a minute, 0.34 percent failure per year, that's one in 300, because it's a third. One in 300 drives will fail per year.

Leo: That's high.

Steve: It's high, Leo.

Leo: Think of how many millions of drives they sell.

Steve: Now I know why I'm getting so many testimonials for SpinRite. Yeah, I mean, one in 300 are going to die per year?

Leo: And even in this case, this wasn't even a drive failure. This wouldn't even have counted there. This was just some error on the data. So, I mean, yeah, it must be even more, one in a hundred.

Steve: I was really surprised that apparently the reliability is beginning to come down. As you say, when you put a terabyte of data, eight terabits on a drive, which drives are now up to, how do you get them all back?

Leo: Well, GRC.com, that's the place to get the answer to that question. I know how to get them back. SpinRite. By the way, I want to thank our sponsor, Astaro Corporation, makers of the Astaro Security Gateway. They're just great folks. We unfortunately had pretaped our show last week so I couldn't mention, they had an event in Toronto last, well, actually it was this week. And I wasn't able to give them a plug, unfortunately, because we had pretaped. But I'll mention future events. It's actually great. They do these events where you can go, and you could try it out, you could see it at work. And the Astaro Security Gateway is a really, really remarkable device. In fact, they wanted me to mention V7. This is a new technology they're launching this month. You may not know about this. I'll get more details on it from the folks. But it's an email encryption, or actually just a basic encryption technology that they're building into this ASG. That's the beauty of it. It's an open source platform. It looks about the size of a router, the Astaro Security Gateway. It's running open source Linux. But because it's such a powerful platform, they can add these plug-ins. It has VPN capabilities, intrusion protection, content filtering, antispam, industrial-strength firewall. It's very high performance. The best thing to do is just try it free. And it's beautiful because sometimes you'll just get new features they just download into the firewall. Contact Astaro at Astaro.com. I shouldn't call it a firewall, it's a security appliance. Or call Astaro at 877-4AS-TARO, and they will schedule a free trial of the Astaro Security Gateway appliance in your business. And we thank Astaro for supporting Security Now!. And I'm sorry I didn't get to mention that event. Feel bad about that. It was actually, as we record this today, it was last night in Toronto, at Lynch Digital Media. Oh, well, next time. Steve, I think we have run out of time.

Steve: We got another good hour.

Leo: And then some. I will see you next week.