Digital Rights Management (DRM)

Description: In preparation for next week's look at how and why Windows Vista has incorporated the most pervasive and invasive system for digital rights management ever created, AACS, Steve and Leo first take a step back to survey the history and evolution of media property rights and the technologies used to enforce them.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-073.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-073-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 73 for January 4, 2007: The next generation of copy protection.

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

Welcome to 2007. And you know, the great news is in 2007 there are no more security issues. There are no more security problems. We don't have to worry about hacking. We don't have to worry about viruses or spyware. So, Steve, we can stop doing this show.

Steve Gibson: So this is our last episode.

Leo: Because they fixed it all; right?

Steve: No more problems in '07.

Leo: Oh, how far from the truth that is. Why, it's a brand new era of spyware, viruses, hacks, exploitation, encryption. And of course, as always, as we've been doing since 2005 – is that right? Yeah.

Steve: Yeah, yeah.

Leo: We will be covering the ins and outs, Steve Gibson and GRC.com. Hello, Steve.

Steve: Hey, Leo. Great to be back. Our first episode of the new year. And just so everyone knows, we're kidding about there being no more Security Now!.

Leo: Do you think anybody believed it?

Steve: I don't think so.

Leo: I can see it on Digg, though. I should really learn. You've got to be very careful what you say these days because it's taken out of context, it gets on Digg, and it gets a life of its own.

Steve: Oh, it's true. You mentioned once, I think you were – I don't know if you were just tired or...

Leo: I was having trouble getting guests, yeah.

Steve: That's right, for TWiT. You just sort of said, well...

Leo: I didn't even say I was going to kill it, I just said I'm having trouble.

Steve: And it was a firestorm.

Leo: I still hear from people. My father-in-law said, "Hey, my friend told me that you're canceling TWiT." Just yesterday he said this. I said I don't think so. In fact, I'm very pleased to say TWiT was named one of the top ten podcasts of the year from Time magazine, so...

Steve: Time magazine.

Leo: Time magazine. Pretty high honor. We're up there with all the biggies.

Steve: Mainstream media.

Leo: Yeah. And most of it is mainstream media. Wall Street Journal and, you know, "All Things.." – or I guess "This American Life," which is my favorite radio show. Anyway, enough of that. And I consider, by the way, that that's the TWiT network more than just any one podcast. Because really TWiT is made up of so many pieces.

We're going to talk today about something that is really new in 2007, a new form of digital

rights management.

Steve: Well, yeah. What happened was, essentially over the holidays there became a great deal of attention focused on a paper written by a guy named Peter Gutmann who is a well-known security researcher – in fact, it's funny. When he and I were corresponding, his email was going into a different folder. And I thought, okay, I know I just got email, where did it go? Well, I had a folder from a dialogue I had had with Peter and one of his coworkers back in 2002 regarding a free cryptographic library that they were making available, an open source cryptographic library. And back then I was talking to him about making use of some of the functions and wanting to get his permission to do so. So I've had a dialogue going back with Peter four years, five years.

And what happened was, he wrote a really interesting paper which I was reading on the plane heading to Northern California for Christmas. Actually it was on December 24. By the time I got to the second page of this thing it had me in its grip. It was fantastic. It's titled basically, I don't remember the exact title ["A Cost Analysis of Windows Vista Content Protection"], but it talks about the effective costs of the new digital rights management technology which Microsoft has put into Vista. And this is something that we've never talked about before. Peter has a very progressive, open source, free speech sort of take on this. But it was really interesting.

So it got me focused on this issue of, wait a minute, I mean, you and I deal with media a lot, Leo. DRM is an issue. We've glanced on issues of digital rights management of the Digital Millennium Copyright Act, DMCA, and so forth, but have never really focused on it. I decided, though, that Vista is – I wanted to do an episode responding and talking, not only about Peter's paper, but with Peter. So he's going to join us in next week's episode about Vista and DRM to talk about the things he said. And also I think it will be fascinating to hear about the reactions to his paper. In the email that he and I have had, in our correspondence, he's just been in a firestorm. Many bloggers have jumped on the things he said, saying that he's wrong. Bob Cringely – remember the old InfoWorld guy, Cringely – basically didn't agree with some of the things he said.

So anyway, it sent me into a research mode for most of the last week to understand what this AACS content protection system is. I wanted to understand the technology of it and basically to do a fact check of what Peter wrote and also to be able to bring sort of a comprehensive view of what this means to our listeners.

Leo: So we'll set that up this week, and then next week we'll talk with Peter, having kind of a foundation for understanding what he's talking about.

Steve: Well, yes. And in fact the reason I want to talk about this, first of all, I think it will be interesting to all of our listeners. And although technically we're about security, no base of listeners more than ours has the foundation to understand this stuff because this is all about crypto and the technologies that we've been talking about, as you said, since 2005.

Leo: Well, and I think DRM falls within our purview, absolutely. Hey, before we get started on understanding AACS, what it is and what it's going to mean going forward, let me just mention, as always, that this podcast starts a brand new year with Astaro. They've sponsored us most of last year, and they've decided to come back for all of 2007. We're really thrilled. It's a good match for us. Astaro makes the Astaro Security Gateway. Now, if you're a small or a medium business, and you're looking for superior protection from spam, from viruses, from hackers, you get a complete VPN, you get intrusion protection, you get content filtering and an industrial-strength firewall, all in a box, a little, affordable, high-

performance appliance, it's really neat. You can contact Astaro to get a free trial, Astaro.com, or call 877-4AS-TARO. You can schedule a free trial of an Astaro Security Gateway appliance in your business. And home users, non-commercial users can download the software from ASG for home use for free, which is pretty neat. It's open source and very, very powerful. Astaro Corporation, Astaro.com. We thank them for their support.

So AACS. What does that stand for?

Steve: Well, it stands for Advanced Access – this has been an acronym soup week for me also. Advanced Access Content System is what it stands for.

Leo: Is it a replacement for CSS, which was...

Steve: Well, it's sort of a replacement...

Leo: That's the DVD encryption.

Steve: Right, a sort of replacement for CSS, although really it's an evolution forward. That's one of the things that I learned during this research is that this is not a completely brand new system. There's been a constant evolution in content protection ever since, well, since the beginning of digital tape stuff happened. You may remember that the audio industry, the recording industry just had a spasm when – it was back in 1987 DAT tape was introduced. Because here was going to be a consumer digital audio tape recording format that would potentially allow consumers to make perfect copies of recordings. And so when we moved into this digital era from the older analog era, things that were already sort of set up to be a problem for the content producers got a lot worse because now there was not this notion of a recording of a recording of a recording. You may remember in elementary school when we had cassette tape recorders, kids would get two cassette tape recorders, hook their connections together, set one to play and the other to record. Remember those old days, Leo?

Leo: Right, yeah.

Steve: And you'd make a copy of some...

Leo: And it would get hissier and hissier with each copy.

Steve: Exactly. And so, yes, that was a violation of copyrights. And so even back way...

Leo: I think there was a loophole, though, wasn't there? I think there was the Home Recording Act, which allowed you to do that.

Steve: Actually that didn't come until after DAT tape. It was, like, four years later. It was in 1992. And actually it was in response to the problem of DAT tape that the Home Recording Act was created. And basically what it did was it required – it by law ordered all digital audio recorders to be equipped with Serial Copy Management System, something called SCMS. And the reason that that happened was, well, first of all what SCMS was, was it allowed you to

make one first-generation copy, but the copy could not be copied. And the reason that happened was that even later, back in '72, the recording industry was worried about consumer tape recorders, as we were talking about, and wanted to tighten up the regulations. But due to the sort of the historical nature of copyrights, the Congress was concerned about just banning all copying. So they put in what was called a "fair use exemption" which allowed individual citizens, like for personal use and for academic use, to make copies, the idea being that those would not be causing economic harm on the content producers.

So essentially what's been going on is, over time this notion of who owns the material really has evolved. The original copyright provision, back in 1788, of the Constitution, it allowed for 28-year protection on books, maps, and charts. And basically it stood that way for about a century, after which time that 28 years was doubled to 56 years. And the notion of printing, which is what they were talking about then, turned into copying because we were beginning to have phonographs and player piano, remember sheet roll music stuff.

But what's happened is, well, the idea was that the overall goal was that the public interest was going to be served, that is, the formal law says that what's good for the public is what we want. So the idea was that allowing anyone to copy anything was not good for the public because that would disincentivize content producers. So the idea was, let's give content producers some length of time in order to have exclusive rights, after which the content will revert to the public domain. And of course that's very much like the patent system that we still have today, where you file a patent that publicly discloses your invention, so for example it's no longer a trade secret, it will be made public, but in doing so you're guaranteed 17 years of exclusivity to that invention in return for making it public, the idea being that that allows other people to build off of your invention during that time, although they have to pay licensing rights and royalties to you if they use it. So originally copyright was a very similar sort of thing.

But what's happened over time, and really unfortunately it looks like it's a direct consequence of the increasing lobbying strength of the content producing industry, they've been lobbying for and succeeding in getting increasingly strong legislation from Congress to create laws which are making this – basically tightening down on individual users' rights.

Now, the flipside of that is, look how the world has changed in, for example, the last 30 years, where back in elementary school kids were plugging two tape recorders together. Now we have hard drives, gigabytes of storage; we have Internet; we have fantastic communications technologies. All of these things, of course, work to make the proliferation of copyrighted material far easier. So those people who are trying to say, wait, you know, we need greater protections today because the world is nothing like it was envisioned back when these original laws were created, I mean, you could argue that they've got a good point. So essentially this is – over the years the legislation has tightened up until, of course, we finally got to the World Intellectual Property Organization, the WIPO treaties.

Leo: Oh, boy.

Steve: Yes. And of course when we signed those treaties we had to have a law to – basically a law on our books to make legal what the treaties were saying. And that's where we got this DMCA, the Digital Millennium Copyright Act, which basically criminalizes and makes much greater the fines involved with basically touching in any way content which has ever been encrypted. And so essentially, technically there's still this fair use provision in the law, but it's gone for encrypted content.

Look at CDs. Now, CDs are non-encrypted, and nobody thinks twice about ripping a CD and sticking it in your MP3 player for your own personal use. And fair use law allows that to be done. You're certainly not supposed to copy the CDs and hand out perfect digital copies to your friends. But unfortunately for the content producers, it's entirely possible to do that because the CD technology was never produced with any encryption. That is, there's nothing there to

prevent that from happening.

So the way the laws have come down is, okay, the DMCA criminalizes the circumvention, even the exploration actually of circumvention into any technology used to thwart copying. So DVDs, even original, first-generation DVDs that are being protected by the very broken CSS, the Content Scrambling System, DVDs cannot legally be ripped and decrypted at all because doing so violates the DMCA, since you are having to defeat content protection which is on the DVD, which is not the case over on the CD side.

So essentially what's happened is, over time the world has changed, computers are becoming powerful, and from the standpoint of content producers, I mean, the creation of the PC is the worst thing that ever happened. These are like little piracy studios that have dropped in price, that you can buy for $500, that all have DVD-ROM burners in them now. So you can stick DVDs in. With the proper software you're able to rip them, decrypt them, and burn copies. This has been a nightmare for content producers. And while they have succeeded in lobbying strongly and passing laws to increase the length of their ownership of properties and to basically make increasingly onerous the threat of breaking these rules, they recognize that laws are one thing, but preventing the copying is what they have to do if it's not going to happen.

I mean, look at filesharing. It's funny, I was talking to Mark Thompson, AnalogX, about this. And I'm not that much into the industry. He's got a friend who is a song author. And in response to my question of, "Mark, has peer-to-peer filesharing and music trading really hurt the industry?," he said, "Without a question." He said he's got a friend who's been watching his royalties dropping year by year because people no longer need to purchase CDs from the store. They can get pretty much anything they want for free in the CD area.

So what's happened is, sort of quietly and behind the scenes, there has been a continuous march of technology moving forward. You mentioned CSS. CSS is the Content Scrambling System which was put onto DVDs from the beginning. It had a number of problems. One is that, due to the export restrictions which we had at the time – you may remember that export restrictions classified cryptography as munitions, and so it was illegal to export anything protected by a key longer than 40 bits. Well, that directly impacted the design – some would say thankfully, those who liked the freedom of doing with DVD media what they want to – it impacted the design of DVD cryptography, limiting it to 40 bits. Also back then the available processing power in players was far lower, so you could argue that players wouldn't have been able to really manage much heavier crypto anyway. So CSS uses a 40-bit key, and analyses of it have shown that only 25 bits of the 40 turned out to be mathematically significant.

Leo: Oh, that's terrible.

Steve: Yes. Well, it's very reminiscent, remember, of the 40-bit...

Leo: WEP.

Steve: ...WEP encryption. You know, it's like, oh, 40 bits is a lot.

Leo: It's enough.

Steve: And it turned out that weaknesses in the encryption caused it to have real problems, as we've covered in the past talking about Wi-Fi stuff. So bottom line is that CSS was protection against casual copying, but it allowed the technology to be cracked and to the point now where

people who want to copy commercial DVDs are pretty much able to do so. So naturally the MPAA, the Motion Picture Association, was not happy about the fact that this protection on DVDs was cracked so badly. On the other hand, the DMCA absolutely guarantees that, since it was encrypted, their intent to protect it is in place.

Now, the problem is, it really does block fair use because individuals by law should be able, were it not for this DMCA ban on copying anything that is encrypted, individuals should be able to copy for their own use. And one of the things that I found really interesting, you may remember this, it was a report that came out maybe about a year ago, and that is that pressed CDs and DVDs are not nearly as archival as was believed. It turns out that there's an oxidization problem that occurs over time. And so our large collections of CDs and DVDs are degrading and have a lifetime that some have measured of maybe 10, maybe 15 years, but not 100. Whereas it turns out that recordable technology, because it doesn't use the same materials at all, CD-R and DVD-R material, has much longer archival shelf storage life. So I have a huge collection of DVDs, commercial purchased DVDs and CDs. And I buy them because I love movies, and I would like to be able to watch these in 30 years. So basically the fact that I'm unable to make personal use copies is a problem that can cause them to basically – for me to lose the value that I had in buying something that I thought was going to last forever. Turns out we don't have that freedom anymore to do so legally.

So over time there's been a series of evolutions in CSS. Informally there's something called CSS2 that never really existed. But there was something called CPPM, which is the Content Protection for Pre-recorded Media. That is what protects DVD audio disks, which I have a few of those, although they never really got off the ground, the idea being that you could take the incredible, never-compressed 7.1 surround sound, basically make a very high-resolution, stunning-sounding, multi-channel recording, which you cannot deliver on a CD because it doesn't have the data rate or the capacity, but you could deliver it on a DVD.

Then there was CPRM, which got a lot more press. It stands for Content Protection for Recordable Media, and it got a lot of attention because the spec when it came out included hard drives, regular ATA hard drives. And people in the industry went nuts because it looked like, if this were implemented in hard drives, then we could start having hard drive content locked. And the CPPM and the CPRM give you protection on a sector-by-sector basis. So the idea would be that we could have arbitrary blocks of sectors locked and encrypted inside the drive in a way that would prevent us, literally, from backing them up. And so there was such a fury that resulted from that that the body that licenses CPRM promised, they vowed never to license any hard drives to incorporate this technology.

And it's worth mentioning now, at this point, that all of this technology is available only under license. It's all protected by intellectual property rights, both patents and trade secrets. Sometimes you can find more information by looking at patents that have been issued to these various companies. But a lot of the stuff is kept also trade secret, where only if you're a licensor do you get the specific crypto algorithms that these things are using, not to mention have keys that are issued to your devices that allow them to participate in these systems.

So sort of quietly in the background this technology has been evolving. There's also something called DTCP, which is Digital Transmission Content Protection, which protects Firewire, the 1394 interface, and USB connections. When protected content is passing over those serial buses, this DTCP comes into effect, and it also has this notion of serial copy protection. There's two bits in there that say you can copy this freely, you can never copy this, you can copy it once, or you can copy it no more. So those are the four combinations that two bits gives you that allows you to govern, or allows the content producers to completely control what rights you have to use this technology.

And then finally there's something called HDCP, which is – actually it's an intellectual property of Intel's. It's High-bandwidth Digital Content Protection, and that's what current-generation consumer TVs and home theater projectors are using, among other applications, but primarily that, the idea being that our content producers have really been extending their reach so that

they're protecting the entire channel all the way from the disk, which is heavily encrypted, through the player, and then even the player's outputs from the player to the screen. There are policies which are bound into the content which allow the content providers to declare whether, for example, they will allow their content to be played over component connections. For years the predecessor to HDCP connections, this digital link to consumer display devices, was component video, so-called RGB video, that many existing home theater systems use. The problem is, it is not a digital technology. It is not digitally protectable. And so, although it isn't being done yet, and no one knows if or when it will be done, anything that is able to deliver this content is able to literally shut down your component video outputs and in some cases deliberately degrade the resolution coming through, if that's what the content owner requests. So they can control whether you get it at all, whether you literally get a fuzzy picture, or whether you get the full resolution that the spec is able to provide. It's just phenomenal how much of this has sort of been creeping along without us really paying much attention to it.

Leo: Seems like they've always wanted the ability to kind of reach into your computer and change how it behaves.

Steve: Well, yes.

Leo: Or even retract stuff if they could.

Steve: Well, that leads us to AACS. AACS...

Leo: Even better.

Steve: Oh, boy. Wait till you hear about this.

Leo: So, now, AACS will be used on what?

Steve: AACS is sort of the end result so far of this constant march towards the content providers obtaining more technological grip on what users can actually do. With the DMCA they got legal grip. I mean, the DMCA has serious teeth in it. The EFF and many free speech activist organizations are very unhappy with it because they really feel that it goes too far. One of the things that has always strengthened our technologies is having them open and able to be examined and discussed within academia. So the DMCA prevents that. You see people saying I can't talk about this because it would be a violation of the DMCA. So it really does go against free speech rights in many ways, like extending itself way beyond just the protection of content. It's protecting anyone talking about the protection of content. So it's a problem. But so AACS is the new system which is part of every next-generation DVD, that is, the so-called high-definition DVD formats, both HD DVD and the Blu-ray DVD.

Leo: Oh, so they both use the same method. They don't have their own methods.

Steve: Yes, they both use the same. All of this comes from a very powerful licensing body. Blu-ray has one step more of encryption, which is one of the things that Sony is trying to sell the content industry in believing because Blu-ray, well, first of all, due to the fact that it's a format which is not compatible with existing DVD production, whereas HD-DVD you're able to retool your DVD production line in order to produce HD-DVDs, Blu-ray requires brand new equipment

from scratch. I mean, you've just got to create a completely new production facility. In return for that, you do get more storage. I believe it's – I'm not quite sure on the least significant digit. But it's like 50 or 56 gigs of storage on a Blu-ray DVD, where HD is 40.

On the other hand, they're also using the latest technology, the H.264, the so-called AVC MPEG-4 codec, which is the generation beyond MPEG-2, which is the compression used for DVD content. That allows them to basically get higher levels of compression. Also H.264 deals with much higher resolution images in a good way than MPEG-2 was ever designed to. Basically MPEG-2 likes 720x480, which is the native resolution stored on DVDs; whereas H.264 can handle the highest current resolution and potentially beyond, which is 1920x1080, at the far extreme end of HD.

So anyway, as I was saying, what Blu-ray offers beyond HD is it can actually contain a replacement copy protection scheme, if the AACS scheme were ever to be badly broken and compromised.

Leo: That's, by the way, what most security and cyber experts told them to do. They said there's no such thing as the uncrackable system. You've got to have backups.

Steve: Well, yes. Now, Leo, you and I have said, I mean, this is one of my mantras on Security Now! is it is not possible to do this. That is, it is not possible to make a system like this work perfectly. And again, as we define security, security has to be perfect because the nature of breaching security is, for example, the weakest link problem. All you need is one weak link somewhere, and you are able to hack the system. Speaking of which, over the holidays there was a great deal of news caused by somebody who posted, I don't remember if it was the Doom9 forums where he first posted. I don't think...

Leo: Yeah, it's on Doom9, yeah.

Steve: I know it's there. I don't know if that's where he first posted. Someone going by the handle of muslix64 announced an HD-DVD backup tool for which he provided the full source code. And on YouTube is a video demonstrating that he has cracked HD-DVD content protection, that is, this latest generation AACS content control system. What he apparently did was he was using a version of Windows, and we don't know which player, but it may have been Version 6.5 of PowerDVD player, which is able to play protected HD-DVD content. He went into the software at some phase of its operation and grabbed the keys. He grabbed the decryption keys and then independently decrypted the contents of the drive, which are just files stored in the standard DVD file format, the UDF format. He took the files and did his own decryption. Now, it's interesting that he posts this in Java because in some of the AACS specs is their samples of this technology is in Java. So my guess is that he read the specs, took the sample code which, you know, the AACS guys made available, basically took the decryption keys out of the PowerDVD player and applied them himself to decrypt the files. And this YouTube video apparently shows him playing one of these files that he independently decrypted. He's playing it outside of the normal protection wrapper.

Well, what he did was not to break AACS at all. What he did was he captured a deep intermediate result. This AACS technology is phenomenal. It involves multiple parties. There's sort of a licensing entity which issues device keys to devices which are licensed to play this content. They also issue media keys to a licensed media replicator, and something called an MKB, which is this Media Key Block. The technology is literally, it's light years beyond CSS. And the Media Key Block uses a very clever system which has been created recently, which forms what's called Broadcast Encryption using something called a Subset Difference Revocation, or SDR. If anyone listening wants to really hurt themselves, put Subset Difference Revocation into Google and then try to understand this stuff. I mean, it is just – it's this amazing tree of

cryptographic keys. And the idea is that it's used for any time you want to broadcast, you want to control the broadcast of encrypted content, and you want the ability to revoke certain keys of receivers of the broadcast, but you want to minimize the overhead of basically sending all of the revoked keys, the idea being that the vast majority of receivers of the broadcast will be licensed and non-revoked. So most of the keys are going to be valid, but some of them need to be revoked. But maybe even a bunch. We're talking about huge, huge numbers.

Leo: If a key is revoked, the player stops working.

Steve: Yes. If the key is revoked, well...

Leo: So it's a way of kind of, if somebody figures out a way to crack it, you just revoke the key.

Steve: Actually it's more than that. It's not that the player stops working. What this thing does is this bizarre broadcast encryption is a way of sending out all of the keys and preventing the revoked receivers from being able to use this technology to obtain their own key. So, but anyway, bottom line is, it's...

Leo: I can't even follow this meta-discussion, let alone...

Steve: I know. It is just, I mean, I've read the thing about three times. I'm kind of beginning to get a handle on it.

Leo: But let me understand, the idea of key revocation is you can no longer play back this content. Right?

Steve: That's exactly right. So here's the AACS technology, and the content protection industry, they are determined not to make the same mistake they made with DVDs. And believe me, they've just gone overboard with this. So disks are licensed. Content is licensed. There are drive certificates and host certificates. There's this Media Key Block which contains this insane subset difference revocation broadcast encryption difference tree technology that allows them – it's not only that they're revoking the key, but because you could imagine that some device that, for example, had been compromised would use somebody else's keys. Anyway, the way this works cryptographically is you are unable to decrypt the content if this Media Key Block is set up in a way that you're unable to.

So get this, Leo. Next-generation players are so burdened down with this crypto, I mean, this stuff, first of all, no more of this 40-bit cipher nonsense. This is AES 128. That's the Rijndael encryption that happened, remember, a few years back that we've talked about. AES is our state-of-the-art crypto. It's 128-bit AES throughout the entire technology. They use sort of AES building blocks to do hashes and for signing and other stuff. They also use full-on public key crypto. They use elliptic curve cryptography as the means for using a Diffie-Hellman public key key exchange between the devices. But this stuff is so loaded down now that, when you insert a high-definition DVD into first-generation players, it takes the player more than a full minute to register the arrival of the disk because the player is sitting here trying to untangle all of this stuff. It's literally, you know, we don't have super-strong processors in these little consumers players, you know, you want to buy it at Fry's or Circuit City or wherever for a reasonable price, they're trying to get the cost down. Certainly we've got much stronger computation today than we did 30 years ago. But still, a full minute just for the player to go through all this work.

Now, the player also has non-volatile memory. And this Media Key Block is serialized. So imagine that somewhere, somebody hacked a player that you owned, and the content industry was tracking this and realized that this player had been compromised, and they wanted to prevent any additional media from leaking out through the player. They're able to revoke, essentially remotely revoke the certificate and crypto capability from that player or all players of that family. And it's not clear what level of granularity there will be, whether for example a certain model of player will have all the same keys, or whether they'll be produced in batches. It's up to the licensor to decide how granular they want to make their license, apparently.

And again, one of the problems we have is that even the contracts and the terms of these things are bound up in proprietary license agreements. There's talk of other remedies, which sound sort of onerous, against people who allow their players or their keys to become exposed. So it's not only that they would be subject to revocation of those assets, but also "other measures," unquote, and nobody knows what those are. So...

Leo: Come knocking on your door, that'd be the measure.

Steve: So when you insert a new HD-DVD into an HDVD player, it goes through all this crypto literally between the drive in the player and the player. Even the bus between the drive and the player's motherboard is dynamically encrypted. And there is public key exchange happening between the device and the player inside to prevent somebody from sniffing the interconnection between the HD-DVD, the physical optical reader, and the motherboard. This thing is, I mean, just locked down.

Leo: Well, they didn't want a repeat of the DCSS affair. They really didn't want this to be cracked.

Steve: Like I said, it's like – it's sort of like, well, how we're paying for what happened after CSS was cracked is that now we've just gone technology heavy.

Leo: Well, but we may not pay if people decide that's too onerous and don't want to do it.

Steve: Well, get this. When all of this public key crypto and an interlock has been established between the optical player and inside of your own DVD player, then the Media Key Block, which is this container of this amazing broadcast encryption subset difference revocation tree technology, it's serialized. The player checks the serial number of the one it has. And after verifying the signature on this to prevent spoofing, if the disk you have inserted contains a newer version of the official Media Key Block, your player will update its copy on the fly to the latest one. That's how revocation is pushed out through the system. So if you were unlucky enough to have the same player that somebody else had that had been cracked and was known to be cracked, playing a newer release of an HD-DVD could render the player inert.

Leo: Oh, interesting.

Steve: It would shut down and no longer be willing to play. Now, in fairness, it's not clear whether this would ever be used against a mass-produced product.

Leo: Yeah, because you'd be putting a lot – I mean, I'd be pretty annoyed if this $1,000 or $500 player I bought stopped working.

Steve: Well, I think it's more than annoyance. I think you'd end up with class-action lawsuits because suddenly a $500 piece of consumer electronics had been deliberately neutered.

Leo: I'm not surprised to hear it, though, because this is where all this stuff has been headed. As I said at the very beginning, these companies want to reach out and get stuff off your drive, or even hurt you for pirating. They really want to be able to reach into your computer.

Steve: Now, unfortunately, as always with security, we're back to the weakest link issue, and that is this HDCP is the High-bandwidth Digital Content Protection created by Intel. This is the way – it's the so-called last mile. It's the link between your HD-DVD player and the screen that you got for Christmas last week, it'll probably have HDMI connections. Anything with an HDMI connector, certainly any consumer product, will have HDCP protection, meaning that it's carrying license keys, and they are revocable.

So just as AACS has revocation – it's funny, too, because the euphemism for this in the industry is "renewability." They want their protection system, their content protection system to have the characteristic of renewability, meaning that it's able to adapt to breaches that are learned. Anyway, the point is that HDCP turns out not to be very strong. It is the weak link. So after going through all of this phenomenal technology to bring the content to you, it turns out that there are known weaknesses which have been published and talked about. But once again the DMCA has put a real pall on any ability to get specific about this as we once would have been because you're a criminal...

Leo: You can't even talk about it.

Steve: ...if you do, exactly, if you lead to this. So it turns out, though, that it looks like this is the weak link, and it's the digital link. So you could imagine that some determined pirates would come up with a crack for HDCP, use an uncracked player, and simply do a digital capture of the decompressed image back into digital form, recompress it, and remaster it. And, I mean, I've got to ask myself, who is it that the content providers are trying to prohibit? I mean, we know there will be pirated, mass-produced HD-DVDs in other places. I have a friend who lives in the Philippines who's visiting for the holidays. And I was talking to him about this stuff, and he's like, "What are you talking about?" He says, "I walk down the street in the Philippines, and there are just racks of Hollywood movies selling for a couple dollars."

Leo: That's the problem, I mean, those are the real pirates.

Steve: Exactly. That kind of piracy. And there's just no way that this is possible. What Peter says – and we'll talk to him about this next week – Peter describes it as requiring the laws of physics to be revoked. Which is sort of his poetic way of saying what I have always been saying, is you cannot do this. I mean, it's not possible to protect because the devices that we have under our control do have the ability to decrypt the content and present it. Otherwise they would be useless. And if there isn't perfect control all the way literally to our retinas, then there are ways to get around this. So, I mean, it's...

Leo: There's always going to be a hole.

Steve: It's fascinating technology. I thought people would find it interesting, as I have over the last week as I've brought myself up to speed on some of these acronyms and details, just how far the content protection industry has gone. The fact that now you've got to wait a minute when you stick your disk into a player, I have heard that the second-generation players are considered very quick because it now only takes about 15 seconds.

Leo: I have to say, on my Xbox 360 I don't notice particularly that it's slow, although there were a lot of complaints early on at how slow these HD-DVD, and Blu-ray particularly, players were.

Steve: Well, and now we understand what it's doing. It's literally, I mean, this is...

Leo: So they just put faster processors in, basically.

Steve: Yes. It is a sophisticated crypto system which is sitting in little HD-DVD players to perform public key crypto on the wire linking, literally linking the optical drive to the motherboard because they just don't want to have any exposed path that would allow people to extract this. But again, Leo, I've never been a filesharing guy. I'm proud to say that, I mean, I have a vast DVD and CD collection. I appreciate the freedom of being able to do what I wish with content that I own. I don't have any pirated content here at all. I buy things easily. But I like being able to convert things to MP3 players or to watch TV or movies on my little Palm handheld. It's convenient for me, so it certainly falls within fair use. But basically, as a consequence of the power of our digital technology, the content providers have decided the greater the barrier they can build to limit that, the better. And in fairness, you have to agree that there are probably people who duplicate commercial DVDs and give them to friends.

Leo: Well, and I guess it's the movie companies' rights to do this. I guess the real question is will consumers put up with it. And will they maybe not buy HD-DVD players or Blu□ray players because of this? Will they maybe stay away from Vista – and this is what we're going to talk about next time – because of all the onerous copy protection and stuff put into it? And I have a feeling as consumers learn about this they might have something to say about it.

Steve: You know, I don't think it's going to matter, frankly. I think, sadly, what we're seeing is we're seeing the end of an era, or as the content producers would say, an error, in the delivery of this media. Now, certainly DVDs will not go away. What we'll see is we will see HD-DVDs and DVDs of the same movies, as we do now, being released. And in fact I just, because I wanted to start really seeing the HD-DVD difference, I bought the "Mission Impossible III" set and of course "Tomb Raider," the first one, because what's not to like about Lara Croft, and Angelina Jolie in HiDef has got to be a good thing, because I want to begin to experience what consumers are going to be seeing.

Leo: I have to say I love it. I've been watching – I watched "King Kong" and "Seabiscuit," and they just look fantastic. In fact, it seems on a good, big plasma screen it seems better than the movie theater. I see more detail. Maybe it's just because I'm closer. I mean, it just really looks great.

Steve: Well, I think probably, exactly, certainly there can't actually be more detail than, for example, on a film. But the fact that you're closer to the screen means you end up seeing – you have a larger frame occupying a larger percentage of your retina. And so in terms of the resolution of your eye, with the screen being close enough, now there are enough pixels that that matches pretty well, so you actually end up seeing a lot more. My feeling is, first of all, when I squeeze something that my TiVo has captured from TV down to 480x320, it's certainly lower resolution than the media content providers are worried about protecting.

For example, there has been some issues about, for example, this notion of constricting resolution, which is what we're going to be talking about next week, which is part of the solution which some players are offering media providers, saying look, rather than disabling non-encryptable outputs, how about if you reduce the resolution? Well, that's going to annoy people who have analog outputs like component video that are specifically, you know, that they got because they wanted to do HD content, and then have the delivery system deliberately make it fuzzy, which is what apparently is going to be possible. But so I have to ask myself, I think most people want to buy DVDs and watch them. Certainly there are people who are unwilling to do that, who would prefer...

Leo: You're saying the people who would care are in the minority.

Steve: Well, and the movies will still always be available on DVD. I don't think we're going to see DVDs die anytime soon, and they've been cracked a long time ago by, as you said, originally by DECSS. And now there are lots of almost push-and-click sort of solutions for that. So...

Leo: Yeah, but they were never easy enough that a lot of people did it. So I think you're right. I think it's a thin layer of people that care about this stuff. And most people are just going to be cows and just say, okay, we'll take it.

Steve: And Leo, what are you going to do with 40 gigs of cracked data? So you decrypt it, and it's 40 gigs.

Leo: Yeah, that's a good point.

Steve: I mean, even on – yeah, I mean, it's much nicer to have it there on a little...

Leo: Just keep it on the DVD, yeah.

Steve: Exactly. Have it sitting on a little disk in the album instead of...

Leo: I guess what I was thinking about is more with Windows and operating systems. If operating systems become encumbered with this cruft...

Steve: We know what word you were going to use.

Leo: Yeah, people are going to viscerally respond. They may not say, oh, shoot, I can't

copy a DVD. But they may say, boy, I don't really like this operating system. I'm not sure why.

Steve: Yes. This is a perfect segue into our next episode because I wanted to create this foundation for next week when we talk to Peter about his paper. I'm going to put a link, and I'm sure you will, too, a link to Peter's paper. He was evolving it rapidly over the first week or two. The last copy I got was December 28. And I looked yesterday, and it was still December 28. So I think it sort of settled down for him. In our correspondence he was saying that he has just been buried under email and responses. So it's really going to be fun to first talk to our listeners about what he has written.

I encourage people to read this paper between now and next week so that you know what we're talking about, you know what captivated me on my plane flight to Northern California by the time I was halfway through the second page, and what motivated me to find out what is AACS. Because what essentially Vista is, is AACS brought to Windows. And this is what Peter analyzes and what we're going to be talking about next week are the user side consequences of Microsoft deciding to turn Windows into a content delivery platform with this much security. Because baby, you wouldn't believe what they have done to Windows.

Leo: Look what they've done to my Windows, Ma. But we'll cover that next week on this very episode, now that we have a little foundation to understand what AACS is up to and how it's going to impact it. And we will have Peter Gutmann join us, which is going to be fun. We don't do a lot of interviews, but this will be fun.

A reminder that you can find this podcast and its 16KB version along with transcripts – this might be a worthwhile one for the transcript – at Steve's site, GRC.com. That's also where you'll find SpinRite, which is the program that Steve created some years ago, now in Version 6, and it's the ultimate hard drive maintenance and, I might add, data recovery utility. Really a great program. You have a letter, I think.

Steve: Oh, I always do. Actually SpinRite was busy over the holidays. This is a really quick one that I really liked, though, because it talks about sort of a different aspect of SpinRite. He says, "Hello there." This is a guy named Dennis. He says, "A few weeks back I started noticing a troublesome sector. One file was stubbornly refusing to be read. Sometimes it worked; most often it didn't. I fired up SpinRite, and once done the file was fully accessible, even though SpinRite found no errors and flew right through the troublesome area. Yesterday it started to act up again, and this time more severe than before. SpinRite to the rescue," he writes. "This time SpinRite immediately discerned that the sector had troubles, and a few seconds into DynaStatting got a perfect read, and subsequently told the drive to swap out the faulty one. Needless to say, the file is now fully accessible. Many thanks, Steve. SpinRite continues to be the best $89 I ever spent."

Leo: So that was a case of an intermittent problem, and SpinRite didn't catch it the first time. But when it did – what is DynaStat?

Steve: What happened was, this sector was on the verge of failing. And so when SpinRite first looked at it, it was able to get a perfect read, and the drive wasn't concerned enough about it either. You may remember that a while ago I talked about how ECC, Error Correction Code technology, is now always being used by drives, and that the ECC correction allows the drive to gauge the size of the error that it's correcting. And at a certain point the error gets so long that the drive decides, oops, I'd better remove this sector from service. So DynaStat is the technology that I first incorporated in SpinRite 3.1. It stands for Dynamic Statistics. Because

SpinRite is actually able to use nonstandard drive commands to read the data from unreadable sectors, which nothing else that I know of does, which is one of SpinRite's tricks, is it performs multiple re-reads and builds a database of different data that it gets from the sector, and is able then to reverse engineer what the original data was. So it was able to basically figure out what the data was, correct it, tell the drive, okay, you've got a problem here, let's put in a spare, and then SpinRite rewrites the corrected data into the newly allocated sector. So that's some of the magic going on just, you know, under the hood.

Leo: Very cool. Well done. SpinRite to the rescue, as he says. GRC.com for that, and of course a lot of Steve's free stuff. How's SecurAble coming along?

Steve: It's done, actually. SecurAble, the utility I talked about two weeks ago, is finished. I looked in my newsgroup, I made a 0.99 version available to the people in our newsgroup. They're reading through all of the text that it encompasses to find typos, and apparently they've found some. So probably in two weeks I'm going to formally release it. I need to get a web page up now in order so that it makes sense to people.

But it has turned out so cool, Leo. It turns out that my tablet PC, my little HP, my TC1100, has a processor that can support hardware DEP. I never knew it because it's turned off. It turns out the BIOS is turning it off, and there's no way to turn it on. So SecurAble told me that my Pentium M can offer me hardware DEP support, even though the hardware won't. So the next utility, which will be called DEPuty, it will have technology to allow you to enable things which your BIOS has disabled.

Microsoft recently got a concession from – I don't know if concession is the right term, maybe an agreement – from all system manufacturers to stop disabling hardware DEP by default. Many of them had been. You had a bunch of users who were using SecurAble found out that theirs also was turned off. In their case, they did have BIOS options they've never paid attention to that allowed them to turn it on. The same thing is true of the virtualization technology. So SecurAble is now telling people if they've got 64-bit capability, hardware DEP capability, and virtualization. So anyway, we've got some good stuff on the way.

Leo: Can't wait. Can't wait. That'll be, what, next week or so that you'll get that out?

Steve: I think, well, I'm working on it now. And so next week we're going to talk with Peter about the consequences of the marriage of AACS and Vista; and then the following week will be our formal release and announcement, and I'll talk about SecurAble.

Leo: Excellent. GRC.com. ShieldsUP is there, too. Lots of other free software. It's really a great resource. Steve Gibson, thanks for joining us. Happy New Year. And we'll see you next week with a discussion of Vista and what's wrong with it, from the point of view of Peter Gutmann, who is a well-known security expert.

Steve: Right. And I want to, again, encourage people between now and then – you'll have a link to it, I'll have a link...

Leo: Homework. Do your homework.

Steve: ...on the show notes. This is a riveting paper that Peter has written. It's written...

Leo: It’s not very long.

Steve: ...in a fun, easy-to-understand fashion. Make sure, though, that you read all the way to the end. When I was reading the December 28 release, it looked to me like he had removed a lot of juicy bits from the paper. It turns out that he moved them to numbered notes at the end. So don’t stop until you’ve read the whole thing. There’s a bunch of really cool stuff at the end, too.

Leo: He also responds to some criticism and so forth, so that you can see the back...