Unbreakable WiFi Security

Description: Leo and I follow up on last week's discussion of the Sony Rootkit debacle with the distressing news of "phoning home" (spyware) behavior from the Sony DRM software, and the rootkit's exploitation by a new malicious backdoor Trojan. We then return to complete our discussion of WiFi security, demystifying the many confusing flavors of WPA encryption and presenting several critical MUST DO tips for WPA users.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-013.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-013-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, lucky Episode 13: Wireless Encryption Part 2.

Steve Gibson is back, the hero of the hour. Did you get a lot of calls about the Sony rootkit?

Steve Gibson: Yeah.

Leo: I mean, whew, this was a big story. We covered it last week. If you missed it, do listen to Episode 12. This is the copy protection scheme Sony is putting on some of its - Sony and BMG Music are putting on some of their audio CDs that is a hacker toolkit.

Steve: Well, and in fact, Kaspersky Lab reports today in their virus news that there is now a new backdoor Trojan program using, that is, leveraging the Sony DRM rootkit to hide itself in users' systems. If it gets into the system - they're calling it Breplibot.b, I don't know why, but it's about a 10KB size file that renames itself sysdrv.exe.

Leo: And as we know from last week's episode, if you have the Sony copy protection on your system, any file named sys will be rooted, rootkitted. It'll be invisible to every tool.

Steve: Right, any file beginning with the sys string just disappears. So we already see - I mean, and we predicted last week that this was going to happen, never having seen one, that this was a serious potential danger for what Sony had done because, rather than only protecting specifically its own files, the authors of this - that were not Sony, they used a subcontractor - the authors arranged to cause anything beginning with the string sys to disappear, including registry keys and any kind of files that are stuck on the file system...

Leo: That's just so sloppy. I can't believe they'd leave that hole on there. Now, how does this Trojan spread?

Steve: It looks like it spreads by spam email messages.

Leo: Oh, so opening an attachment.

Steve: Tricking people into loading it.

Leo: Okay. So don't download files or...

Steve: And it apparently opens a back door on the user system.

Leo: Don't download files from unknown sites, open attachments. Be very careful. Now, here's a question for you, and a number of people have asked me this. There are some anti-spyware programs that claim to detect the Sony rootkit. Kaspersky must be able to. If it's a rootkit, how can they do that?

Steve: Well, they're able to - well, for example, the Sony rootkit is easily detected. You could simply rename a file to sys.

Leo: Oh, yeah.

Steve: If it disappears, you know you've got the rootkit on your system. You don't even need to use RootkitRevealer, as we were talking about now several times, in order to do a scan of your whole system.

Leo: Yeah, somebody, shortly after we put out the podcast, mentioned that and said he's created a file on his desktop called syscanary, like the canary the old miners used to take down. If that...

Steve: And if it ever disappears...

Leo: If it disappears, you've got trouble. So, okay, so it's easy to detect. Is it easy to remove?

Steve: That's the problem. Now, Sony - there's been, you know, we were part of the initial uproar at this time last week. In fact, you know, we did our podcast a day early because we wanted to make sure this message got out as quickly as possible. Sony has responded to the pressure. They're doing some butt-covering PR spin, saying that there's really nothing wrong with it, but we'll put something on our site that people can use to remove the hiding behavior. The DRM technology stays there, but the hiding behavior at least will be - it'll be shut down.

Now, the other revelation since last week is that Mark at Sysinternals has confirmed a report that he heard. And I have not yet myself - I've ordered one of these CDs that I'm going to be infecting myself with here in a couple days because I want some firsthand experience of this myself. But the Sony technology is also phoning home. It uses the user's Internet connection on the fly, when they're listening to any of the disks that they've purchased using this built-in player. It sends a message back to Sony saying that this particular song or album is being played. Apparently this is for some sort of, like, banner rotation technology that it has to present something to the user. But the problem is this is classic spyware phoning home behavior. It is not disclosed by Sony. And in fact, Sony specifically says that's not being done, yet it's been found in packet capture traces. And Sony's saying, well, but if we're doing it, then we're not keeping any of the information.

Leo: We're not doing it, but if we were to do it, we wouldn't keep it. How can you trust a company that does that? That's terrible.

Steve: Oh, it's so bad.

Leo: All right. So this isn't the primary topic of our show today, but we did want to kind of update you all on that. And so what should we do? I still am kind of baffled about all that.

Steve: Well, I think it's a function of how concerned individual users are. You know, our goal here with these

podcasts is not to tell people what they have to do ever, but to say, look, here's the truth about what's going on. You decide for yourself how concerned you are. As long as somebody knows that this content-enhanced Sony CD technology is installing technology on their system which does allow known Trojans to hide themselves, well, okay, if that's what they want, I have no problem with that, as long as they know.

Leo: Right, right.

Steve: So, you know, we do know that you can go to Sony, you can submit your email address to them to get a link for a remover which will remove this from your system. So you've got to go through some...

Leo: You can't get it any other way? You can't...

Steve: ...in order to get this removed.

Leo: You can't just go to XPC Aurora and download it? You have to...

Steve: I guess - I think you can do that, too. And get this removed from your system. Then, if you ever make the mistake of installing one of these Sony audio CDs into your computer, as you said last week, Leo, hold down the Shift key.

Leo: Right.

Steve: Or, if you're a more security-concerned user, you might have already disabled the CD autorun feature in your system, which otherwise causes this thing to present you with a EULA. If you ever see the End User License Agreement because you forgot to hold down the CD, decline the installation and, you know, play the CD normally, or hold down Shift when you put it in to prevent this thing from being reinstalled.

Leo: Right. Okay. It's too bad. And I hope, you know, there are lawsuits, class-action lawsuits. I suppose some aggressive district attorney in some state or country might actually go after them for...

Steve: I think there is some governmental action I heard in Ireland somewhere. And there's an ambulance-chasing class-action-happy law firm in San Francisco that's filed against Hewlett-Packard and Toshiba and everybody you can imagine. And they're, you know, rolling up their sleeves to go after Sony now.

Leo: Okay. So, you know, and I have to say I'm actually pretty disappointed with Sony's response to this. They have minimized consistently. They've lied, obviously. Well, it sounds like they've lied anyway about the phoning home issue. And they're really not taking responsibility in a way that I would hope they would.

Steve: Well, it's certainly been a good object lesson for other people...

Leo: Yes.

Steve: ...who will hopefully not follow in Sony's footsteps.

Leo: Yes.

Steve: And, you know, I don't think we've seen the end of this. I'm going to take a look at the CD myself. I may have one suggestion next week, in next week's podcast, which you and I will be doing from Toronto

again.

Leo: That's right, yeah.

Steve: Otherwise, I think this issue is behind us.

Leo: All right.

Steve: Anybody who's interested, by the way, can just put "Sony rootkit" into Google and stand back.

Leo: You'll find plenty about it.

Steve: Yep.

Leo: Well, yeah. And it was kind of timely because we had just talked about rootkits. So I'm glad we had talked about them because then, lo and behold, it became an issue, so. But we had also started a conversation about protecting yourself on a wireless network, and that's a very important conversation day in, day out, as well. So let's get back to that. When last we spoke, we pretty much debunked the notion that MAC address filtering had any impact on security. SSID hiding, useless. WEP encryption broken and next to useless. It sounds like the best way to do this is WPA.

Steve: Yes.

Leo: In fact, the only real way to secure a wireless network is with WPA.

Steve: Yes. Just to clarify the issue of SSID and MAC filtering, because I got a lot of mail from people after I said, you know, it was not useful for security, complaining about my position on that. So...

Leo: Wait a minute. Wait. How could they complain about your position on it? What you were talking about is factual.

Steve: Well, yeah, but...

Leo: Do they dispute that at all?

Steve: Well, I guess maybe the problem is what I mean by security. MAC address filtering and SSID hiding, and also changing the SSID from the default, which typically is Linksys or D-Link or Netgear or whatever, those are useful for preventing inadvertent use of your access point by a neighbor who just has, you know, not implemented any security themselves. Many people were of the feeling like, hey, you know, encrypting my home network is a pain because I have...

Leo: More of a pain than MAC address filtering? No, that doesn't make any sense. In MAC address filtering you've got the MAC address of each device you have to enter in. You enter in the password once in WPA encryption, and that's it.

Steve: Well, but, for example, if, you know, what I'm citing from people is they've got friends who come over with a wireless laptop who want to use their access point.

Leo: Yeah?

Steve: So I guess, you know, somebody who's into this is able to add their MAC address of their wireless NIC on their laptop to their permissions list on their access point. They know how to do that flexibly and so forth. They don't have to modify their friend's laptop at all.

Leo: Just give your friend the password, and he can log in.

Steve: I know. I know.

Leo: It doesn't - it's not logical. These people are not being logical. You either...

Steve: No. What I want to clarify is that...

Leo: All right.

Steve: ...the use of MAC address filtering is not secure, nor is SSID hiding or changing your SSID from the default, because both of those are easily obtainable just by sniffing the air.

Leo: Right.

Steve: However, they are useful to prevent inadvertent use by a neighbor of your access point. So...

Leo: I have an analogy for this, Steve.

Steve: Okay.

Leo: Let's say you don't want to lock your door because you want your kids to come in and out of your house freely. So you don't lock your door. You have no security. But just to kind of discourage burglars, you put a big sign out front that says you have an alarm system. Now, in fact, you don't have an alarm system, and the door isn't locked. But you've put a sign up that says you do. That's that kind of security. I think it's not particularly logical. If you ask me, give your kids a key and lock the door.

Steve: Well, again, it's not secure. It prevents...

Leo: It's pretending to be secure.

Steve: Well, maybe we need another word. I mean, it's very weak authentication is what it is. And authentication is different from security.

Leo: Okay.

Steve: It's not authentication of your wireless devices that cannot be broken, which is to say even that can be breached. But it's weak authentication, which is better than none if you want to prevent your neighbors from inadvertently using your system. But it should never be confused with security, and that's what we're going to talk about with WPA.

Leo: So let's say, how to protect your system for real, not by putting a sign up that says "it's secure, really..."

Steve: Right.

Leo: ...but actually securing it. How do you do that?

Steve: As we talked about when we talked about how badly broken the whole WEP original legacy encryption for WiFi was, I was talking about all the different ways that it could be compromised, to the point where, you know, there are now - there's, like, competing hacker tools that run on Linux platforms, that allow people to sniff your traffic, induce your access point to spill keys at a much faster rate than it normally would, that allows them to be analyzed in order to crack your key. So WEP encryption, again, it's better than no encryption at all. It does provide a much better barrier than leaving your system wide open or even protected by MAC address filtering or SSID hiding, but it can be cracked.

The reason I make this point is that WPA, even the weakest form of WPA encryption, if it's done properly, is absolutely uncrackable as long as no one gets your key. The WEP is so badly broken that, when they thought, uh-oh, okay, let's really fix WiFi security seriously this time, they got heavy-duty security experts involved, and they created a next-generation encryption technology called WPA. It has a number of different ways it can work. And unfortunately it's an acronym soup that gets very confusing very quickly. But specifically, WPA, sort of all an end-user needs to really appreciate is that, if you use a really good passphrase - and we've talked about passwords and passphrases before - a really good passphrase, you are virtually uncrackable. Now, there's TKIP, which is a Temporal Key Integrity Protocol, which basically changes the keys often enough that existing encryption, that is, the RC4 encryption that was in the early WiFi can now be used safely. There is more industrial-strength WPA, also called 802.11i, also called WPA2...

Leo: And sometimes I've seen it as Enterprise WPA, as well.

Steve: Exactly. Well, and that's even...

Leo: Is that the same thing?

Steve: ...a little bit different.

Leo: Oh, okay.

Steve: Because that's why this is all so confusing. WPA2 uses AES encryption, which is the new NIST encryption standard. So it doesn't use the RC4 encryption. Some people think, oh, well, that's better. The fact is, RC4 encryption is an extremely strong cipher, absolutely strong enough, as long as it's used correctly; and WPA technology uses it correctly. The reason we're still using RC4 is that there's a very good chance that older technology systems can be upgraded with - older routers can be upgraded to WPA security, even though they've got older hardware. The problem with AES encryption, which is this next stronger level, is that it's much more hardware and processor intensive, and so only newer hardware that was designed with this technology from scratch will probably be able to run it.

Leo: So give me a shopping list, in order, from least secure to most secure. And I presume you would choose the most secure you had as an option; right?

Steve: Well, maybe. But, you know, from all the feedback we've received from users, people are very sensitive to any sort of inconvenience. Well, we know that inconvenience and security are always fighting each other. It's like...

Leo: Right. I have to say, though, my experience with WPA is it's much less inconvenient than WEP was. It's a...

Steve: Well, okay.

Leo: It's a simple passphrase. You enter it once, and most implementations you don't have to enter it again, and...

Steve: Well, that's true, except get a load of this. It turns out that passphrases are much less secure than they seem.

Leo: Oh. Oh.

Steve: Typical passphrases are, you know, per character of a passphrase, due to the fact that case is not changing randomly, that is, uppercase and lowercase, that passphrases are normally not highly mixed with letters, special symbols, and alphabetic, and that there's generally a lack of randomness in a passphrase, the typical strength of a passphrase is 2.5 bits of security per character.

Leo: Compared to a random string?

Steve: Well, compared to a byte, which is 8 bits. So we're used to thinking in terms of a character as being of 8 bits' worth of strength.

Leo: Right.

Steve: So for example...

Leo: So it's less than a third as - it's a third as strong.

Steve: Right. So, for example, if you had a 20-character passphrase, it turns out that's only good for 50 bits of encryption.

Leo: Again, because there's some organization. The best password or passphrase is totally random.

Steve: Well, exactly. So what this means is that there is an attack which WPA, well, which pre-shared key WPA can be subjected to. And you're right. We have to talk a little bit about what this means. The easiest to use, most practical and workable encryption is called PSK, Pre-Shared Key, WPA. And that's what you've been talking about, Leo, where you simply make up a really good passphrase once. You assign that to your access point, to any wireless equipment you have in your home, and you're done.

Leo: It's very easy.

Steve: Now, the enterprise...

Leo: Now I'm worried it's not secure.

Steve: Right. The enterprise stuff adds another level. It uses a technology typically known as "radius

technology," where there's another server somewhere that authenticates the user and dynamically creates keys for them so that each user has a separate key sort of assigned on the fly. One consequence of normal pre-shared key WPA, this PSK WPA, is that all devices in your environment will be using that single pre-shared key. So they're able to cross-decrypt each other's traffic if they wanted to.

Leo: Ah, I see.

Steve: Meaning that, in a corporate environment, if you had a bad employee...

Leo: Right.

Steve: ...and the whole corporate access point was using the same pre-shared key, employees would be able to spy on each other's traffic.

Leo: Right.

Steve: Now, in a residential environment, we know that's not going to be a problem.

Leo: So this is where you have to kind of be aware of what your needs are and choose appropriately.

Steve: Right.

Leo: So in a business you should probably not use PSK, but in a home environment PSK would be acceptable.

Steve: Well, and in a business environment you're going to probably be spending more money or have a bigger budget; or, you know, in a serious corporate environment you've got, you know, a whole IT staff that are going to be doing this.

Leo: Well, but also in a corporate environment you still have the advantage of you enter it once and your system remembers the passphrase; right? I mean, you don't have to re-enter it every time you log onto the base station, do you?

Steve: Oh, absolutely. In a corporate environment, with a radius-based server and dynamic key assignment, the user is authenticated...

Leo: Each time.

Steve: ...against this major - this main central server, and then keys are dynamically assigned to the access point and the user on the fly. So it's not burdensome in any way.

Leo: Give us, if you can, before we go much farther, I'd just like to understand all the flavors...

Steve: Okay.

Leo: ...all the players involved. And then, if you would, can you talk about the pros and cons of each?

Steve: Yes. Okay. So with WPA we have either a static, pre-shared key; or, in corporate environments, keys which are being assigned by a centralized server where the users authenticate themselves with their own password and credentials, then the server creates the keys used for their connection. No users at home or even in a small office environment are going to see that or be involved with it; but I wanted just to say that, you know, it exists, and it's there, and it's super high-grade security.

Leo: And the purpose of that is to keep people from snooping on each other within the network.

Steve: Correct. Also, if you had an ex-employee...

Leo: Right.

Steve: ...who left and had the knowledge of what that pre-shared key, a single global pre-shared key was, that would create a vulnerability also.

Leo: Right.

Steve: So in a corporate environment, this WPA using a central server for, like, key distribution solves cross-user snooping and the problem of keys not expiring from people being fired or leaving the company and so forth.

Leo: Got it. Okay, that makes sense.

Steve: So in a home environment, everyone is going to be using a single pre-shared key, which is completely safe as long as the passphrase that generates the key is safe. And that's how we'll wrap up our dialogue here in a few minutes.

Leo: Okay.

Steve: But first I'll say that, so, we have the issue of a single key or dynamically assigned keys. Everybody in the home is going to be using a single pre-shared key. Then another aspect of WPA is which encryption technology is being used. Older hardware, which is not as strong, will tend to be using the RC4 encryption, which has been made safe by changing its keys all the time using something called TKIP, the Temporal Key Integrity Protocol. TKIP makes RC4 safe where it wasn't safe before in WEP legacy-style encryption. Alternatively...

Leo: Okay.

Steve: ...newer hardware that is stronger might be capable of using a different cryptography technology called AES. So, for example, my new Belkin router does offer me AES encryption. So if XP, if the XP client that I was using also supported AES, I might choose to use it. It is more processor-intensive. Technically it will be putting more of a load on my computer. I haven't chosen to use it because TKIP is absolutely safe enough. It is a more efficient technology and protocol. And if someone came over with a slower laptop who I wanted to briefly allow to join my network, now TKIP is for sure what they're going to be able to use within this WPA umbrella.

Leo: Okay.

Steve: So that really wraps up the choices.

Leo: And I guess the key is you've got to kind of know what your security needs are, and you can choose. But for most home users, any form of WPA would be good enough. Yes?

Steve: Yes. Exactly. So the lowest common denominator will be WPA with a pre-shared key using TKIP technology encryption, which drives RC4. Like I said, it's an acronym gumbo.

Leo: Take notes, kids.

Steve: Okay, so...

Leo: Yes.

Steve: The last thing that is important, and this is critical, is passphrase quality. The reason it's critical is WPA is subject to what's called an "offline attack," meaning that someone could sniff your traffic and only needs a little bit of traffic to sniff. They don't need a lot. They then take that home to a big computer and run an offline cracking utility, which basically it does a brute force, or dictionary, attack against your passphrase. So because it's possible to do this, to put as much time or energy as necessary, you know, since you're bothering to do WPA anyway, you know, it absolutely makes sense to choose a good passphrase. And what that means is somehow come up with just a jumble of arbitrary special characters. You're able to, with WPA passphrases, you can use anything printable, you know, asterisks, dollar signs, you can look like a comic book swearing person - upper, lowercase, numbers, you name it. And use the full length. A passphrase can be 63 characters. And that's what I'm saying. This is not somewhere where you want to type in a sentence that you like to use. That can get cracked offline. You want just a nightmare jumble of junk. And then you just use copy and pasting in order to paste the same thing into each of your machines at access point. And when a friend does come over, you paste this jumble in, they can't memorize it.

Leo: Right.

Steve: So, you know, before they leave, you delete that from their wireless adapter, and it's safe just by obscurity. There's no way anyone is going to - even you are going to be able to memorize this 63-character hodgepodge of just static.

Leo: Now, let me ask another question. And this, I think, is really where the criticism comes from on what we were talking about last time with MAC address filtering and so forth. People say, how real is this threat, anyway? Aren't we kind of spreading a lot of fear unnecessarily? How many people are getting hacked?

Steve: I don't know how to respond to that because, again, our goal is just to explain the technology. So it's important for people to know that WPA is subject to offline cracking. So that if they were in a situation where they thought they were secure using a few English words strung together as their passphrase, maybe it's useful for them to know how that can be broken, and that it really can be broken.

Leo: Right.

Steve: That, you know, if I were in their facility, and I wanted access to their system, I could get it, even though they've used WPA.

Leo: And then you can decide, folks, whether you really want to worry about this or not. I mean, that's - I guess that makes sense.

Steve: Yeah. I think that's...

Leo: You need the information.

Steve: That's our, you know, that's our position. I know from the people who write to us, Leo, that there are people who do think we're going overboard. I mean, you can imagine, I got a lot of mail when we were talking about listening to keyboard clicking noises.

Leo: Well, we know that that's silly.

Steve: But it's possible.

Leo: We just want to let you know, I mean, we thought - that was a case of, well, I think it's interesting. I don't think we ever implied that somebody was going to do that to you.

Steve: I'm not worried about that.

Leo: On the other hand...

Steve: Believe me, I do have an extremely strong WPA passphrase that I can't remember. It's in a file on my computer. And when I need to set up a new device, I copy and paste it into the device. There's no way I could even type it again. But it's absolutely never going to get cracked. The reason is that passphrase ends up getting hashed 4,096 times into a 256-bit master key. 256 bits is way long for a master key. So my point is, while you're doing WPA security, if it's okay with your lifestyle to have a key that you can't remember, but because you can't remember it, that demonstrates how strong it is, then take the time to do it once, and you never, never need to worry about it again.

Leo: So then our recommendations, if I can summarize, are use - certainly use WPA. If you're - let's, maybe, well, I have to put that little codicil at the beginning. If you are concerned about WiFi security, use WPA because it works. Use a completely random password of 64 characters. That's the maximum?

Steve: Actually 63.

Leo: 63. And that's the most you can use. And randomize them. And don't use a phrase, even though that's easy to remember. But since you're just cutting and pasting, you don't need to remember it.

Steve: And it only has to be done once.

Leo: And you don't have to worry about Temporal Key, TKIP, because that's really more for a business situation where you want to provide security between people who are on the same network, or maybe protect yourself against former disgruntled employees. In a home environment, that's probably not necessary.

Steve: There actually is some firmware that can be downloaded into the Linksys, that WRT54G, you know, that nice little router that a lot of people...

Leo: Everybody has, yes.

Steve: ...that are using and running Linux, that does have, like, a little mini radius server technology in it, if somebody really wanted to get into this in a home environment.

Leo: You could implement Temporal Key.

Steve: Not a typical application.

Leo: Okay. And if you don't use WPA2, you don't worry about that.

Steve: Nope, not at all.

Leo: Simple WPA is fine. All right. Okay. And again, folks, if you want to put a sign on your front lawn that says "This house protected by guard dogs," and keep your door unlocked, be our guest. We're not telling you not to. We just want you to know what the risks are when you do it. Right?

Steve: Or how about a little sign in the window that says, "Using strong WPA with a passphrase you will never figure out."

Leo: "So go away." And then you can just leave it wide open because who cares? All right, Steve. Hey, it's always good to talk to you. And I think that this was important. And we apologize to those folks who wanted to hear more of the wireless encryption and were less worried about the Sony rootkit for a little interruption, our little intermezzo last week. But we did think that was important, too.

Steve: Well, yes. People really wanted guidelines for how to really lock down their security. I mean, I'm responding to the mail that I get.

Leo: Yeah.

Steve: People wanted this, so that's it. That's the story. Next week, unless something happens, we're going to finally talk about VPN technology...

Leo: Okay.

Steve: ...to be safe no matter where you are using wireless.

Leo: Right. And we will come to you from Toronto next week, of course, via podcast as always. For more information, visit our show notes at GRC.com/securitynow.htm. You'll also find two versions of Security Now! there, the normal 64KB version and a 16KB version for those of you with slower download speeds or less file space, as well as transcripts. And I think it's great, Steve, you've got them in text and PDF form so people can read what we say and understand it. Sometimes it helps to read it in addition to listening to it.

Steve: And there's one thing I meant to say that I forgot to say, but it's very important. WPA may not be available on your platform.

Leo: Oh, yes.

Steve: It's only officially available in XP. There is a free WPA client software that runs on all versions of Windows - 95, 98, and on - that used to be from a company called Wireless Security Corp., that apparently McAfee recently acquired. But if you put "free WPA client" into Google, it'll take you there. And I'll have a link to that on the Security Now! page on GRC. And also, Leo, I'll send it to you for the show notes.

Leo: Great.

Steve: Because it will allow people who have a WPA-capable router, but who are running OSes that do not have a WPA client to, for free, add WPA technology to their system. And that's very important.

Leo: That's nice. And as we said when we talked about WEP, if all you have is WEP, WEP is better than nothing. You know, use that. But just understand the risks that you're running.

Steve: Exactly.

Leo: And, you know, next week we'll talk about using VPN. And even if you're using WEP, VPN can be very handy in securing your system.

Steve Gibson, thanks for joining us. Our hearty, deepest thanks to the folks at the AOL Radio Podcast Channel who not only broadcast this podcast, but give us the bandwidth so that you can all download it easily and freely at AOLmusic.com. I'm Leo Laporte. We'll see you next time on Security Now!.