
# Listener Feedback Q&A #33

**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-128.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-128-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 128 for January 24, 2008: Your Questions, Steve's Answers, #33. This show and the entire TWiT broadcast network is brought to you by donations from listeners like you. Thanks.

Well, here it is, ladies and gentlemen, the one show where we're not going to mention Heath Ledger, we're not going to mention the stock market crash, we're not going to mention Bernanke's drop of the interest rate or the Federal Reserve Board. This is the show where you don't hear any of that stuff. This is the show where we talk about security. Steve Gibson, hello, how are you today?

**Steve Gibson:** Oh, Leo. Well, it sounds like your voice is back to full strength here.

**Leo:** It's cracking a little bit. Every once in a while I go tenor.

**Steve:** Okay, well, our listeners are now prepared.

**Leo:** I was practicing singing high notes a little earlier on, and I actually was able to hit notes I haven't hit in a long time. Isn't that odd that a cold would change the register of my voice? It's a little weird.

**Steve:** You sound fine here, so...

**Leo:** You never got it, did you.

**Steve:** No, no.

**Leo:** Knock on wood.

**Steve:** Exactly.

**Leo:** Do you have any wood in the fortress of security?

**Steve:** Underneath the Formica I think there must be some. I'm not sure if that qualifies as wood, though. That's like that pressboard stuff that we use to kind of...

**Leo:** I've never been to your lab. But I just think, I feel, it's probably very modern and, you know, kind of masculine.

**Steve:** Oh, it's definitely masculine. When my ex wandered off, I covered over the fireplace with bookcases because I needed more shelf space.

**Leo:** I knew it.

**Steve:** Yeah, you can't cover up your fireplace when there's a wife around. That does not go over really well.

**Leo:** Nowadays they're saying don't burn wood, don't burn wood, it's making people sick, stop burning...

**Steve:** Oh, and I mean, I'm in Southern California. I just had to turn the AC off here on January 23rd so that we didn't have the background sound of the air rushing through our podcast.

**Leo:** Steve, there are people listening who just had 37 inches of snow.

**Steve:** So my point is, I hardly need a fireplace down here.

**Leo:** I guess you're right. It's the last thing you need in Southern California. So this is a Q&A episode. Every other episode now, and on even episodes we do listener feedback. But we've also made a pledge to give you the latest security news. Anything going on in the world of security out there?

**Steve:** Well, one or two big things. But more than last week, it was a rather quiet week.

**Leo:** Thank you.

**Steve:** Yes. The really significant news is that there is now a remote code execution exploit of the horrible Microsoft Windows TCP/IP problem, the vulnerability that we talked about last week.

**Leo:** That's the one they patched Patch Tuesday of this month.

**Steve:** Yes. So it's absolutely been patched. But it is, you know, I was saying last week there is just no question this is going to be an Internet worm because there are still so many machines that are not being patched, whether it's because they don't pass the Windows validation test and so they're no longer able to be patched, as they used to be sort of, you know, pirated copies either way, or who knows why these machines are not getting patched. And there is now, it has been found - and in fact, in some of the security discussions, Microsoft was apparently mitigating the severity. I know that's hard to believe. But they were saying, oh, it's really going to be difficult to exploit this. Well, [buzzer sound], no. It turns out, no, it took one week. You know, so...

**Leo:** Since zero-day exploits are the norm, that was difficult. Took them a whole week.

**Steve:** Right. So it is now in the wild. And I expect that it won't be long before we see this demonstration of the vulnerability turned into a worm that works on propagating itself for whatever purpose around the 'Net. I mean, the good news is that most of these 'Net-wide worms have just been created for the sake of proving that they could be done. You know, the original ones, of course MSBlast was different, it had a destructive payload aimed at Microsoft. But Code Red and Nimda, they just sort of wanted to see how long they could live and how far they could go, so they weren't doing much, although you really would expect now, with bots being as popular as they are, that we might see a worm based on this with an express purpose of creating new zombie machines. So that's something we never saw really before. You know, sort of general...

**Leo:** When you say the exploits are out there, there isn't yet a worm exploit, just a script's exploiting it from a web page?

**Steve:** Right. It's easy to say that it isn't yet a worm because the whole industry will know the instant a worm happens. I mean, it will be another major event where it's like, okay, suddenly everyone's routers are getting pinged with this nonsense from a worm trying to propagate. I mean, we'll all know when that happens because it'll explode on the Internet.

**Leo:** Well, and remember the last time, it must be the last time there was a worm of this potential was Zotob. And that hit CNN and a lot of people. But one good thing is that, when these things happen and they get a lot of publicity, people respond by changing their security policies.

**Steve:** Right. That's a very good point. So each one of these events does have the nice side effect of further maturing people's understanding that they need to keep their Windows systems patched.

**Leo:** And they seem to dampen, because of that, it dampens down. So next time's not as bad.

**Steve:** Right.

**Leo:** One hopes.

**Steve:** Well, although, I mean, this is exactly - oh, I'm sorry, I see what you mean. People have learned to patch, so they're now going to be keeping their machines in general more secure because they've realized this is a real problem.

**Leo:** And as an example, I'm sure that the companies that got bit by Zotob now run internal firewalls on all their machines because they mostly got bit when people brought laptops, infected laptops into the network behind the firewall. And so as these things happen, people kind of build defenses. Of course it's always closing the barn door after the horse is gone. But it at least keeps the horse from running out that door again.

**Steve:** Right. And the second bit of news is, and I saw this when I turned on my little Mac in order to set up our Skype session today, Apple has confirmed and patched a rather serious QuickTime vulnerability.

**Leo:** Yes, I downloaded it today, yeah.

**Steve:** Which exists in all versions of QuickTime prior to version 7.4, which the industry has now moved up to. Everyone who turns on their Macs will get this. And but it affects both - we referred to this I think last week because this seemed familiar to me when I saw the patch coming in. It's like, okay, this is what we were learning about last week for the first time because this is both OS X and Windows. And the problem is that it's a remote code execution vulnerability which can take hold of a machine anytime you run a QuickTime video, an image file, or a stream. So pretty significant. And that's been patched, too. So the good news is people who are using Macs and - what's the - I don't even know about QuickTime auto-patching for Windows.

**Leo:** It does the same thing. It's very similar. And it happened on my Windows machine. In fact, there was an iTunes update at the same time. So I opened my Windows machine, I think this was yesterday or the day before, opened my Windows machine, it said there's a QuickTime patch and an iTunes update, would you like to download those. And it looks very similar to any kind of automatic update. If you've installed QuickTime, unless you've explicitly turned it off, and I don't even know how to do that, it should do that automatically.

**Steve:** Yeah. I do know that I get the little QuickTime "Q" sitting in my tray all the time. It's like, eh, I don't know what that's there for.

**Leo:** Wish it wouldn't do that. Everybody's does that, but it always annoys me. You know, it's like, oh, that starts it up quicker. Yeah, thanks.

**Steve:** I think they just want a little chunk of my screen.

**Leo:** It's an ad.

**Steve:** Exactly, it's an ad. So that's all we really have.

**Leo:** I've turned that off on my system. I think you can actually turn that off.

**Steve:** Oh, suppress the icon? Oh, I'm going to go searching for that, then. That will be a good thing.

**Leo:** Definitely worth doing. I like it best when, if you right-click on the icon in the system tray and say "Exit," it says, okay, but we'll come back unless you don't - do you not want us to start up automatically ever again? And I think QuickTime is one of the programs that actually has that what I consider good behavior.

**Steve:** Yup, that's a good thing.

**Leo:** All right. So that's our update.

**Steve:** So that's all we had there. I do have a fun, short SpinRite tale to tell.

**Leo:** Yeah, I thought you might.

**Steve:** This one was - when did we get this, we got this one in - Aaron, who is, well, it's a sort of interesting story. He says - I was looking for the subject line. He said, "Just a SpinRite Story." He said, "Back in 2003, long before I had heard of SpinRite and Steve Gibson, my hard drive crashed in my Dell desktop computer with all of my digital pictures on it. I heard clicking noises, so I was 'sure,' he says in quotes, that it was a total hardware drive failure. Dell send out a replacement drive. I reinstalled, and I was able to reload most of my stuff from a month-old backup. So I lost a month's worth of precious family photos. The data recovery software I tried" - clearly not SpinRite - "could not help. So I called for estimates from some data recovery companies." Clearly he really wished he had his month's worth of family photos. He says, "I just couldn't afford that, so I put the drive in a box for the next four years."

**Leo:** But at least he saved it.

**Steve:** Yes. He says, "...just in case."

**Leo:** That's great. That's like having your - that's what Walt Disney did. With his head. Just in case.

**Steve:** Yes, somewhere in cryo storage right now.

**Leo:** Yeah, just in case, down the road, something comes along that could fix your hard drive.

**Steve:** So he says, "In early 2007, parens, {three computers later)" - this guy goes through computers quickly. And he says, "I learned of SpinRite while listening to a weekly," oh, he says, "while listening to a newly discovered security podcast."

**Leo:** Hey.

**Steve:** "I had a current computer problem and decided to try SpinRite. It fixed my 2007 problem easily, and my mind was then drawn to that old hard drive in a box in a drawer. Could it fix that, I wondered. I connected that old drive to an old computer that was lying around and let SpinRite run for the next 26 hours. Well, after four years locked in a failed hard drive, we finally got that month's worth of pictures out of the hard drive."

**Leo:** Hey, yeah.

**Steve:** "The moral of the story is, regular backups are a good first line of defense." And he says, parens, "(Remember, I did have a month-old backup.)" He says, "And SpinRite is a great second line of defense. Thanks, Steve.

**Leo:** That is a nice story. And I love the idea that he put his drive in cryogenic storage just in case.

**Steve:** It's like, it's very much actually like Walt Disney. But, well, maybe someday something will come along that will be able to recover these.

**Leo:** And, you know, it's a good bet.

**Steve:** Yeah.

**Leo:** Even for Walt Disney I think it's a good bet. I mean, I'm not going to do that, but I would do it with a hard drive.

**Steve:** Sure.

**Leo:** Of course SpinRite's been around 20 years before he had the problem, he'd just never heard of it.

**Steve:** Exactly.

**Leo:** I had to laugh when you said that because, I mean, it's like you hear about it in 2003,

wait, this is...

**Steve:** Yeah, what year is it?

**Leo:** Yeah, really. Anyway, let's get down. I have some great questions for you. Are you ready to talk about listener feedback?

**Steve:** You betcha.

**Leo:** We start with Eddie in Watsonville, California. He confesses he shortened his key: Dear Steve, I've been a listener of yours for probably a year and a half now, converted my wireless network to WPA some time ago, and used one of your 63 random printable character Perfect Passwords to do it. That's GRC.com/passwords. All was well as long as I only had computers that I could copy-and-paste the password into. Then I bought myself a PSP, a Sony PlayStation Portable. After six failed attempts - oh, dear - at entering the WPA key, I decided I didn't really want to take my PSP on the Internet anyway. Oh, it's a pain because it doesn't have a keyboard. You have to do it all, oh, gosh, I can't...

**Steve:** And I still don't have my iPod Touch on my WiFi. I mean, I hear that it's got WiFi, but I can't type my key into that thing.

**Leo:** That's why I don't use the long...

**Steve:** I know.

**Leo:** Then for Christmas I received a WiFi desktop Internet radio. It supported WPA. I knew I had no chance of entering that ungodly key correctly, so I went back to GRC.com/passwords, copied the first 24 characters of the random alphanumeric string. Still took two attempts on the radio and three on the PSP, but - and the good news is you only do it once - they're all happily on the network. My question is - and this is a really good question - how much less secure is 24 random alphanumeric characters than 63 random printable characters? I understand that the 63 is, as you might say, phenomenally more secure, but I'd like a number. Would it take a hacker decades instead of millennia, months instead of centuries? I would imagine even the most determined hacker would give up after only a few days. Just how much security have I given up? Great question.

**Steve:** Great question. Okay. So here's what happens. When you put a passphrase into WPA, any passphrase a user puts in is run through a sort of an overkill hashing process. It takes the passphrase and the SSID of your network and the SSID length, and it hashes - it concatenates all that, and it hashes it 4,096 times, over and over and over and over and over, into a 256-bit result. So the key that is actually used by the various devices on the WiFi network ends up actually being a 256-bit key. So the source of the key is the passphrase and the SSID and the SSID length. So as we've discussed before, the attack on what's called a "preshared key," which is what this is, is trying them. It's just a - it's a brute-force attack. Anybody who has access to your network, that is, like receive access, as we know, is able to receive the SSID of your system if it's not turned off. And if it is, then that's part of the hash anyway since other devices wouldn't know what it was.

So the only unknown in this hashing algorithm is the passphrase. So the attack on this technology is just brute force. You start with maybe all the words in the dictionary, and essentially put a word in the dictionary through this overkill hashing, this 4,096 hashes of this, to produce a trial 256-bit key, and then check to see whether that works on the network. And if not - and actually you're able to capture payload from the network and see whether this key is able to decrypt the payload, which then tells you that it would work on the network. So that's why this is a so-called "offline attack." You're able to capture some traffic from the network, take it home with you, or to your Cray, and just pound on that data, trying every possible passphrase.

So 63 random printable characters is the most that the specification allows a user to put in. Now, 63 random printable characters, assume that we had like a 7-bit character set, so we're using most of the printable ASCII. Well, 63 times 120 - I'm sorry, 63 times 7, which is the number of bits in 128, actually, is 441. So you're taking - if you used all 63 possible character length and hashed that down, you'd be hashing 441 bits down to 256. So you're sort of starting with more entropy and reducing it to 256. In theory, there may be other so-called "hash collisions," that is, there might be some simpler phrase that would also hash down to the same resulting 256 bits. But, you know, it's a secure hashing algorithm. Collisions are going to be minimized. And so it's still going to require a brute-force attack. The current wisdom is that 20 characters is, eh, right on the borderline of what would be feasible for a brute-force offline attack against WPA. So you really don't want to use fewer than 20 because that begins to border on not secure enough.

**Leo:** Now, remember, though, in order to crack your WPA somebody has to sit on your curb. They have to be within radio distance of your base station.

**Steve:** No no no. That's the point of this being a fully offline attack.

**Leo:** Oh, they can just capture a bunch of the stream and then drive off and work on it.

**Steve:** Exactly. And that's what I meant, that's what I meant when I said they could take it home to their Cray.

**Leo:** Of course, you did say that. I just wasn't paying attention.

**Steve:** And so, and just pound on it offline. And/or do a parallel attack, or use a distributed network of PCs, I mean, or...

**Leo:** Somebody would have to be pretty determined to do this.

**Steve:** Yes, I mean, exactly. So, well, or you would be targeted, they would want to get onto your network specifically, as opposed to, for example, someone wandering down the street looking for open WiFi. This is certainly a much higher level of attack than that. And your typical home user is probably not going to be targeted by somebody who really wants to get onto their network. However, a corporation certainly could be.

So Eddie was suggesting that he's used 24 characters. That's probably good. One of the things you do not want to do, and our answer sort of touches on this, is you do not want to leave the SSID default, nor do you want to leave it blank. Because one sort of future-oriented attack on WPA will be precomputed hashes. That is, if you knew, for example, you had a Netgear WiFi,

and there was a default Netgear SSID, it would be possible to do a different kind of attack. Rather than having to put the passphrase and the SSID and the SSID length into this function and hash it like crazy - and in fact that's the reason they've used 4,096 is they want to slow down this kind of attack by forcing 4,096 hashings of this in order for it to be computationally intensive in order to make a single guess.

So but the problem is, there are things called "rainbow tables," and I don't think we've ever really talked about rainbow tables. They are essentially precomputed hashes. So the reason that the SSID and the SSID length were added to this was specifically to prevent a precomputation attack where all of the, for example, words in the dictionary, or maybe starting with A, then Ab, then Ac, then Ad, then Ae and so forth, basically precompute all the possible hashes that result from common words, and then quickly apply those against offline packets in order to crack somebody's encryption. So my point is that, if you leave the SSID default, then you're potentially opening yourself to a precomputation attack, if that starts happening.

**Leo:** Okay. So if I do a 20-character...

**Steve:** Eh, I would say 24. What Eddie happened to settle on at 24 is probably safe. I would say nothing less than 20 is safe. And I have a - I found a nice page on the 'Net with a link to a discussion of this, if our listeners are interested and want to go into a little bit more detail than this, sort of without me interpreting what this page says. It's pretty technical. But there is a link in this Episode #128 show notes to a page that discusses the issue of this attack on Wireless Protected Access preshared keys.

**Leo:** Okay, very cool. Now, when you say "safe," that's a very relative term. I mean, I use, I mean, I'll be honest. I just use what normally, you know, what would be considered a normally kind of strong password, which is something I - but memorable. It's probably only 10 characters.

**Steve:** I would say you absolutely want it not to be in a dictionary. I mean, and so that's...

**Leo:** It's got punctuation, it's mixed case and punctuation. But it's memorable for me. And but it's not 24 characters.

**Steve:** Yeah, and let's hope that no one desperately needs to get into your wireless network.

**Leo:** And nobody does.

**Steve:** I don't think so.

**Leo:** By the way, I met somebody at Macworld Expo, guy who does a podcast, Dan's Mathcast, who says he's used the math - he'll take a little clip of Security Now!, like that early part there where you were talking about powers, and he'll use that, and then use it as his mathcast to talk about that math issue. So...

**Steve:** How cool.

**Leo:** ...good work on the math there. When he first said that, I thought, oh, no. But he says, no, no, you guys are always good. Don Sherman in Clawson, Michigan is looking for a shorter route: Steve, he says, I'm a graduate student in engineering and a huge fan of the show. I just finished listening to the most recent Listener Feedback episode. It occurred to me that on several occasions I've heard you say you need three routers to safely employ WEP and WPA without allowing - both WEP and WPA without allowing any nefarious activity on the WEP side to compromise the WPA side of things. Is there any reason why you need to use a router and not a switch to split the two networks? If so, please let me know, as this is how I have my network set up. I cannot use WPA with my TiVo boxes.

**Steve:** Okay. Let's review briefly this idea of chaining routers. The idea was that you could have your outside Internet connection go to Router #1, and that would be a wireless router running WPA or WEP. And then you would chain it to a second router which was also wireless, running WPA or WEP. Now, the problem is, if the inside router is the insecure one, then it is potentially able, that is, somebody who cracks WEP, and we know how easy that is now, remember it's less than a minute to do that now. If someone cracks that, then due to the fact that it's possible to make upstream connections through a router, which of course is how the Internet works, we're all downstream of our routers, and we're able to make upstream connections through the router. That allows somebody on the inside, that is, on the inner router, to connect to devices on that outer level router because upstream connections are permitted. So that's why it's not safe to have an insecure network chained off of your secure network.

Now let's swap the routers around so that now the outer router, that is, the one connected to the Internet, let's make that one the WEP, the insecure WiFi router, and our WPA router where we have all of our crown jewels and our high-security WiFi due to using WPA. That's the inner one. Now the problem is that all of the precious, super secure network traffic goes out through the inner router to the outer router, which is the insecure one. The problem is, as we've discussed before, in the face of ARP spoofing, which is well mature now and developed for Ethernet networks and for Ethernet WiFi, it is possible for - it would be possible for a wireless attacker to convince the inner router, the secure router, that its IP is the gateway, so that all of the precious Internet traffic on the inside would route through an attacker's machine on its way out to the Internet. So there is a, if you assume that ARP spoofing could be present, then it is not secure to have the insecure router upstream of the secure one because ARP spoofing absolutely allows essentially man-in-the-middle traffic rerouting.

So it is not safe to chain an insecure and a secure router together in either order. The only thing you can do that is safe is to have two routers that are joined by a third router.

**Leo:** So you need the NAT. You can't just use a switch.

**Steve:** Well, no, actually. So what the outward-most router in a three-router configuration would be doing really is just giving each of the interior routers an IP. So to answer Don's question, if his ISP has given him two IP addresses, then you absolutely could use a switch.

**Leo:** I see. You have to have two segments, basically.

**Steve:** Well, actually you have to have three segments. You've got your insecure LAN, your secure LAN, and then a third little mini LAN that only has three devices on it. It's got the switch, and then it's got the two routers. And the reason you're safe from WEP there is that, I mean, the only real attack that's possible would be an ARP attack. And you say, well, wait a minute, why can't I still spoof ARP in order to fool the outside interface of the super secure

router? The reason is ARP never crosses a router. ARP is specifically used for local area networks. No router will allow ARP to cross across from its LAN side to its WAN side. So the only secure solution would be either to use three routers, or as Don has asked, if his ISP is giving him two IPs, then he could use a switch to connect those two routers.

**Leo:** Got it.

**Steve:** And be completely secure.

**Leo:** Got it. All right, good. Jeremy in St. Petersburg, Florida, wishes he had more choices: Hi, Steve. I was a bit disappointed over having to pay $72 for my VeriSign credit card security key, due to $24 overnight shipping being the only option. Hmm. They could have just put it in an envelope. But I've received my key, and I agree it is a really slick piece of technology. I ran into one snag, though, that I hadn't heard mentioned on the podcast when you and Leo were discussing them. The problem is with eBay and VeriSign's PIP site. Both allow you to only have a single security key associated with your account. This is unlike PayPal, which allows multiple keys. Because of this, I can't leave my football at home in the office and have my credit card in my wallet. I have to pick one of the IDs, and only one, to use with eBay and PIP/Seatbelt.

I wrote an email to VeriSign support and got a very nice reply from Gary Krall, the technical director of the PIP program. He confirmed that VeriSign, like eBay, has no plans at this time to support multiple security keys. VeriSign I can understand. They have a higher, you know, high priority things on their plate. But doesn't eBay own PayPal? How can one site support more than one key, but not the other? Anyway, this means I basically had to disable my football on eBay and PIP so I could use the cooler credit card key. My football will still get me into PayPal, but that's it. That actually was the experience I had, too.

**Steve:** Yup. I just wanted to let your listeners hear Jeremy's pain because we've all had it, too. I don't understand why eBay hasn't followed suit. It is certainly the case, as we've discussed before, that the VeriSign VIP technology now supports up to five credentials registered to a single account. And so the user of up to five credentials is free to use whichever one they want. And when you submit the query, the authentication, to VeriSign's authentication system, it'll check the specified input against all five, up to five possibilities. So, and PayPal does this. But eBay and VeriSign themselves don't. So I just wanted to make sure that our listeners knew that, just for the sake of making sure they understand that.

**Leo:** Yeah, yeah. But, you know, I keep the football for use on PayPal, which is frankly still where I use it the most. And I just use the card, just as this guy does, on Seatbelt. I don't use eBay that often, but that's fine.

**Steve:** Yeah, and after all, the football's only $5, so it's not like he was having to, you know, end up deciding to scrap his $72 cost credit card side.

**Leo:** You think it's a security reason for that, or just an implementation issue?

**Steve:** I don't see any security flaw in having multiple credentials. I mean, I just think eBay just doesn't care, hasn't gotten around to it.

**Leo:** Moving right along, Marcio in London, UK, wonders whether - as opposed to, I don't know, London, Iowa - wonders whether IBM is spamming him: Hi, Steve and Leo. I have received a spam email, I know, nothing abnormal with that. It was just another "replica watches" spam. Obviously neither my email client nor my company's email server filtering policy seems to be finely tuned in, other wise that wouldn't have slipped through. The curious bit, though, and the reason I'm writing, is the sender's address is kasey@ibm.com. Could there be a trick, changing the sender's address? Or is it the case that an IBM server or computer could be bot-infected? Please let me know what your thoughts are.

**Steve:** Well, it's interesting. I get sort of a little background flow of email like this, asking about strange spam sources. So I wanted to...

**Leo:** Well, people could get spam from TWiT.tv because I know that's used sometimes by spammers.

**Steve:** Oh, and GRC has been also. Essentially what's going on, Marcio, is that the content of email, which contains the From and Subject and To and other headers, is completely separate from the - and that sort of inside the envelope - is completely separate from the protocol used by SMTP servers, that is, Simple Mail Transfer Protocol, to move that email payload from one machine to another. So from random computer A to random computer B, which are email servers, a sort of an opaque content will go from one server to the other. So there is the ability to trivially spoof the sender of the email just by putting anything they want to, and typically something credible. I mean, Leo and I have both been targets because we're credible companies, and people might think, hey, email from GRC, how strange.

**Leo:** Hey, but I've got to tell you, I think sometimes it's randomly chosen because I get questions on the radio show all the time from people saying, hey, what's going on, you know, I just got a bunch of bounced emails from a company saying I'm sending them spam. What's happening? Same thing.

**Steve:** Right.

**Leo:** So I think sometimes they do it for credibility. I mean, IBM.com clearly for credibility. But sometimes it's just - they choose it from random from a mailing list.

**Steve:** Yup, that's probably the case, Leo. So anyway, to answer your question, Marcio, I am sure that IBM machines and servers are not infected. It's just it's so simple to spoof the source of email, that is, the sender. Now, we've talked about this in the past. If you dig down into the archives of Security Now!, we've talked about email headers and how they can be interpreted in order to determine the true source of email because that's not spoofable. And so there is a way to determine what machine connected to your email server in order to send it a piece of email by following the headers back. But it's not just a matter of looking at the From address.

**Leo:** Well, and of course that's why there have been these various moves towards email authentication, which essentially is sender authentication. And if that were to go through, if they were able to figure out a way to do that, it'd just reject email that doesn't have an authenticated sender, and pretty much all spam would go away. But, you know, because the email system was never designed for that.

**Steve:** Right. We can hope for that day.

**Leo:** That's why three years ago Bill Gates said, oh, I think spam will be a thing of the past next year. The problem - and because Microsoft had an authentication scheme. Problem is, nobody's really been able to agree on what scheme to use.

**Steve:** Right.

**Leo:** Thomas Bonham has a question for Mac-friendly Leo: Hi, Steve and Leo. I'd like to know if you know of any good encryption software for OS X, 10.5. That's Leopard. I'm unable to use FileVault because of the fact that I have HFS+ with case-enable on the computer. It doesn't like that. I'd really like to be able to encrypt the whole drive. But for now I'd be happy just to have one folder encrypted all the time. What I'm looking for right now is something like TrueCrypt for the Mac. Any ideas would be great.

**Steve:** Leo?

**Leo:** Hmm, that's a good question.

**Steve:** No kidding, there isn't something that's on the tip of your tongue that...

**Leo:** Well, what surprises me is that TrueCrypt has not been ported for the Mac.

**Steve:** Right.

**Leo:** But it hasn't. That's a very good question. I don't, I mean, you can use PGP, but that's a commercial - I guess there's a noncommercial free version. I don't, you know, I don't know. I'll have to do some research. I don't know of anything, believe it or not. Because most people use, if they're going to do the encryption, they use the FileVault, which is very similar to the system-level encryption on Windows.

**Steve:** So essentially the Mac does provide a built-in solution.

**Leo:** Oh, yeah.

**Steve:** Which works for most people. And so that's probably kept people from doing something redundant.

**Leo:** I think that's possible, yeah. I'm not sure - he says he's using HFS with case-enable. That's interesting. I didn't know that you couldn't use FileVault in that case.

**Steve:** And what's "case-enable"?

**Leo:** Case-sensitive, I guess.

**Steve:** Oh, okay.

**Leo:** But that's what I, I mean, that's what everybody uses. I think, Thomas, you should investigate why you're not able to use FileVault. Apparently there is - I'm looking. Somebody has been looking at a port of TrueCrypt. So I hope at some point - Bruce Schneier is saying, I'm reading his blog, he's saying, you know, I hope at some point there is a TrueCrypt for Mac. And of course, remember, Mac is BSD UNIX. So there are a lot of UNIX, you know, command line level encryptors you can use from the UNIX command line. But that's going to take some cobbling. It's not as easy to use as TrueCrypt. Boy, I wish they would port it. I don't know why they haven't. Maybe there's some issue. I don't know of anything. And if anybody does, love to hear from you, and we'll mention it on a later episode. But Thomas, all I can say is, the problem with FileVault, it's like BitLocker. It encrypts your whole home directory. So it isn't as flexible or as powerful or as useful as TrueCrypt.

**Steve:** Right.

**Leo:** Matthew Reeves of Alpharetta, Georgia really wants to delete his files: I'm a lawyer - a lawyer. No, I'm a loyal Security Now! listener, and I'm so thankful it exists. Well, thank you, Matthew. I remember once hearing you and Leo speak of a secure file deletion utility. I don't remember its name. I went to search the transcripts, but I couldn't find a way to do so. That's probably true. So my question is, what is the name of the utility? And my question is, can the Security Now! transcripts become searchable, if they aren't already and I missed it?

**Steve:** Okay. To the last part, it is on my shortlist of things to do. We've had a lot of requests for that. It is possible in the meantime to get Google to do a limited search, since the transcripts are all being Googled. And so by using the advanced search features you're able to restrict Google to a domain, and I think even a tree of files, in order to have it say, look, you know, find hits for these phrases right here. So that can be done. But I'm aiming soon to have, finally, a search facility that is GRC-wide up and running. As for secure deletion, there are a gazillion various sorts of file shredders and things. It turns out, though, that most people don't do it right.

**Leo:** Oh, really.

**Steve:** Interestingly, yeah, interestingly enough, you may remember that, like I'm sure you will, Leo, in the old days, we were being told that NT was a C2-qualified OS. It met some government standards for security. One of the things that is required for that is that the operating system be very careful about re-use. That is, for example, when memory is allocated to an application, Windows NT, 2000, XP, Vista, everything in the NT path or family will always zero the memory page. In fact, one of Windows' background processes, when it's not doing anything else, is just rummaging around, filling memory that's not allocated to anything with zeroes.

**Leo:** What? That's really cool.

**Steve:** Yeah, it is really neat. Now, similarly, disk space is zeroed, but it's not zeroed upon deletion. It's zeroed upon allocation.

**Leo:** Oh, that's interesting.

**Steve:** So what's interesting is, if you delete a file, and say that you then, you also deleted it out of your trash, well, it's been released, but we're all familiar with various utilities that are able to undelete files. Similarly, anything that worked offline, like if you shut Windows down, it turns out that that file data is still available on the hard drive. It's not until a program is being given sectors for its use that NT preemptively zeroes it. So what's important here is that everything that isn't in the process of being reused is left the way it was.

So it turns out, though, that things are even trickier because, if you encrypt a file, what NT does is it, because of the way the file system works, sort of a journaling file system, we've also heard how NT - like for example the file system integrity can survive power failure or the plug being pulled out of the hard drive and other things - NT is careful, for example, not to remove a unencrypted file which you're in the process of encrypting until it has been successfully encrypted. Once it is successfully encrypted, then NT unlinks the unencrypted version, but leaves it on the hard drive. So you can have copies of unencrypted encrypted files...

**Leo:** Not good.

**Steve:** Exactly, still lurking around. The same is the case for compressed files. It's compressed and encrypted, and there's one other class. Oh, and even, well, the EFS system works in exactly this fashion. So anyway, the point is that our good old friend Mark Russinovich has solved this problem. Of course we know that Sysinternals was purchased by Microsoft, and so there are - his utilities, the Sysinternals utilities are now available and linked through Microsoft's site as opposed to his. There is a program he has called SDelete, "S" as in "Secure." It's just SDelete. If you were to Google, you just put "SDelete Sysinternals," it'll take you, first link is Microsoft's page. On our show notes page we've got a link to the Microsoft page discussing Secure Delete, SDelete utility. And to the downloadable ZIP file.

It's just a - it's a small command-line utility that understands exactly how NT works. And it uses the defragmentation API in order to find the actual physical pieces of a file which you're trying to securely delete, and it goes out and zaps them before freeing them back to Windows. So it does it right. Many so-called secure delete utilities do not do it correctly. So, but we can trust Mark to have figured this out and done it right. And it's got a couple other cool things. If you were worried about, for example, now that you understand the things you deliberately encrypted or things you deleted may still be lurking around, you can give it - it's a command-line utility. You can give it, I think it's a -Z option, and it will go out, and it will scrub all of the current free space on your file system. So basically you could just run it now, and it would deal with any history of stuff that you were hoping was gone, but may not be gone.

**Leo:** Interesting. Mac has a secure-delete command in the file menu, but I wonder. I bet you it's not erasing slack space. And, I mean, but at least it would zero out the file, and I presume all copies of the file. But slack space is a big issue.

**Steve:** Right.

**Leo:** We may have mentioned this, as well. When you want to erase the whole drive, for

instance you're giving away the computer or you're giving away the drive, there's a free program, open source program called Darik's Boot and Nuke.

**Steve:** Yup, DBAN.

**Leo:** DBAN, which makes a bootable floppy or CD-ROM. And the reason you want a bootable floppy or CD-ROM is you don't want to be doing this from within Windows if you want to wipe the entire drive. Mark's utility is for individual files. But if you want to wipe the entire drive, DBAN, you just - it's very simple. Google DBAN, and you make a bootable floppy or CD-ROM. And then it says, you want to erase the whole thing? Yes, please, yes, yes, yes. And then you finally can zero it out. I just was looking at the TrueCrypt page. Interesting. TrueCrypt 5, which is scheduled to be released this month, will include OS X support.

**Steve:** Yay.

**Leo:** So it's going to be completely cross-platform, which is nice. You could make, for instance, an encrypted USB drive or external drive in Windows and be able to read it on OS X. Plus they're going to do a GUI version for Linux. So that's a major improvement. There hasn't been a release of TrueCrypt since May. Obviously they're working on this TrueCrypt 5. So watch for that. Who knows, maybe by the time you hear this it'll be out.

**Steve:** Well, and Question #8 from Michael Daniels...

**Leo:** Applies to that?

**Steve:** Yes.

**Leo:** Well, we're not there yet. We'll get there in a second. Steven Barrett in Round Rock, Texas would rather switch than fight: I know that it's really difficult to use another operating system that you're not brought up on. But why not just use something other than Windows? This probably sounds like another "Windows sucks," or "I'm a Mac fanboy that's irritated at everyone not using Macs," or "Linux is superior to everything because it's open source." But honestly, why not?

**Steve:** Well, Leo...

**Leo:** That's a question for you because you, despite knowing more than probably anybody what's wrong with Windows, at least security-wise, you stick with it.

**Steve:** Yeah. I guess I thought this was interesting because I do - this is another question that comes up over and over and over is people say, gee, Steve, you know, you're spending all this time talking about how horrible Microsoft Windows is and all the security problems it has, blah blah blah. Why not, I mean, why would you not have moved off of Windows?

**Leo:** Right. You can't.

**Steve:** I was going to say, my real answer is, this is where the problems are.

**Leo:** You're not allowed to.

**Steve:** So this is where I am, exactly.

**Leo:** I think we talked about this before. You said, hey, if I weren't doing this, if I were retired, I probably wouldn't. And I use Windows for the same reason. Actually, I use Windows maybe more than that because, for instance, I use Windows for Adobe Audition, which is my editor, my audio editor and recorder of choice. I have not found anything as good on the Mac. And so I use Windows because I need a Windows app.

**Steve:** Well, that is exactly my real answer, aside from the fact that this is where I have to be, is virtually anything, I mean, okay, we were just talking about TrueCrypt, not yet on the Mac. But it's been on Windows for a long time, I mean for years, because we talked about it a long time ago. And so my position is - and I talk to people who are frustrated that the thing they want to do is not available on their non-Windows OS, but it is on Windows.

**Leo:** Well, but it goes both ways. There are many things you can do on the Mac that you can't do on Windows.

**Steve:** Dare I say SpinRite.

**Leo:** Good example. Perfect example. But there are - and it's the same, I mean, there are things you can do on Linux you can't do, I mean, there's Rsync. Windows does not have Rsync, which would be a really nice thing to have. There's lots of things I can think of that aren't on any given platform. But, you know, to address his issue, I personally think that people get over-attached to their operating system. Remember, you may love your operating system, but it doesn't love you. It's just a tool.

**Steve:** Well, and Leo, you know, I buy a lot of software. And so in the same way that I'm now buying eBooks for my Kindle on Amazon, and I'm sort of locked in there, I mean, I've got a huge investment way beyond just the Windows OS in all the stuff that runs on Windows.

**Leo:** Well, that's a good argument for open source. The sooner you open to open source, the sooner you'll be free from those shackles, economic shackles. You know, I use Windows, Mac, and Linux. I probably use Mac more than Linux or Windows. But it's more equal than most people probably think. And I'm happy with all three. Use the tool for the job you're using, you know, you're working on.

**Steve:** I think that's exactly right. As we know, I'm a FreeBSD UNIX user for things where UNIX serving is the best solution. And there are, you know, I tried to use Windows as a news server, a Usenet style, NNTP. And it's just, oh, it's really bad.

**Leo:** No, all my web serving is done from - we use Red Hat Enterprise Server. I have two servers, dedicated servers. Nobody else is using them, just me. And they're both running RHE. And I manage them. They're not managed. I manage them myself. And absolutely, I mean, these servers are rock solid and have been for years. And it's been, you know, once you tune them, once you figure out, you know, how to get everything just so, man, they just run, you know, tens of thousands of requests a day, day in, day out.

Michael Daniels of Dallas, Texas - Question #8 - wonders if TrueCrypt is truly cryptic: Hi, Steve and Leo. I'm a longtime listener of the show. I've followed you guys since TechTV, when Steve would occasionally appear on The Screensavers as a guest. Thanks for the podcast. Keep up the good work. I have recently started to keep my files mobile by carrying a 120-gig hard drive around with me. However, after a short period of time I thought, this is stupid. If I lose this drive, anyone can access my files. I looked around, found TrueCrypt, an open source encryption utility. I was wondering what you use, and if TrueCrypt is indeed any good. I apologize if this question's been asked before, and I haven't made it through all the show archives yet.

You know, I just got a USB key from Corsair that came with TrueCrypt on it. I was so pleased.

**Steve:** Yeah. And the answer, Michael, is TrueCrypt is really nice.

**Leo:** It's the best.

**Steve:** Yes. We did an entire podcast on it, so I wanted to aim Michael and anybody else who didn't hear that back to the archives for our Episode on TrueCrypt [Episode #41] where we take a very close, an extensive look at TrueCrypt, the functions it supports, the way its crypto is done, I mean, the really clever little special things that TrueCrypt is that really make it our solution of choice.

**Leo:** Yeah. And boy, I'll tell you...

**Steve:** And soon to be on the Mac.

**Leo:** When it's Mac, oh, man, I'll be happy. And that's actually a very good use for TrueCrypt is an external hard drive, or any external device that you carry around with you. This Corsair memory, you know, it's a USB key. They have 16-gig, they have 32-gig, I mean, this is basically an external hard drive. Absolutely you should be using TrueCrypt if you're putting private information on there.

**Steve:** Yup. In fact, we're going to do an episode also shortly about IronKey, which we talked about briefly last week, which many people have asked about. And the founder and chief architect of IronKey is going to join us...

**Leo:** Oh, good.

**Steve:** ...to talk about his inspiration and to clarify some of the details of the technology. But, I mean, it really is, it's a very, very nice-looking system.

**Leo:** But I think, you know, given - you know, it's hard to learn all the ins and outs of TrueCrypt. But once you figure it out, it's just as secure, right, I mean, it's just great.

**Steve:** Oh, it's spectacularly secure, yes.

**Leo:** Don Hebert of Burbank, California wants more pixels: Hi, Steve. I noticed in a photo that you use three monitors. So does Bill Gates. Hooking up two monitors is easy, but how do you hook up three monitors? And how do you use them? Where was that photo? I didn't see you in a photo.

**Steve:** There's a photo at the top of my page at GRC.com. I think you just do GRC.com/steve or stevegibson, I don't remember which, or maybe either. And there's a shot that was taken by a Newsweek photographer many years ago of me sort of grinning and leaning...

**Leo:** Well, that was probably three different computers, then.

**Steve:** Well, no, it was exactly the same computer and monitors I'm sitting in front of now. That's why I got a chuckle out of our other questioner, who said he's, you know, in three years he's gone through three machines. I tend to hang onto mine for a long time. I mean, they get kind of old and creaky. I'm still using my Win2K box with three monitors. And to answer Don's question, you simply plug in video adapters. And at least in the case of Windows, it will see your video adapters, and you're able to arrange the monitors logically into one large screen and essentially just drag Windows back and forth among the various monitors.

**Leo:** We used to talk about this a lot on The Screensavers when it was a little more difficult.

**Steve:** Right.

**Leo:** I mean, there was a website that said which cards worked together and stuff. But since XP it's been a lot - well, you're doing it on 2000.

**Steve:** Yeah. And 2000 supports multiple monitors just fine. To answer...

**Leo:** It's best if you have three of the same cards, though, yes?

**Steve:** It really doesn't matter.

**Leo:** Oh, okay.

**Steve:** It's a little confusing. I should tell you, I do this a lot. So I've got many machines with, like, a hodgepodge of screens on them. It's a little confusing if the monitors are different sizes because then they don't really, like, stack next to each other well. And there's, like, some weird ozone area, a rectangle that you can't get to sort of off to one side. But...

**Leo:** You want a rectangle. You don't want some arbitrary [indiscernible] box.

**Steve:** Right. And you can do strange things. I mean, you can stack them vertically or horizontally. If you had four you could put them into a square configuration. And there is a cool little utility, UltraMon, that I like and that I've had running in my tray for many, many years which allows you to assign hotkeys to just make Windows jump to different monitors. So, for example, I have Ctrl-1 moves whatever is the current window to the left in a sort of a circular fashion, or Ctrl-2 moves the current window to the right. So it's easy for me to just quickly move a Window off to one side.

The way I use the monitors is I generally sort of have things in different positions. I just like having more screen real estate. I mean, I'm able to work with a laptop with only one screen. But when I'm settled down into Mission Control here, I do have, like, reference windows. For example, when I'm writing code, and I need to kind of keep an eye on the Windows API, which is so extensive that it's impossible to memorize it all, I'll have the API reference upon my left window so I'm able to just glance over at it. And I don't want to cover up the editing window that I'm typing in in order to see the API reference and vice versa. So there are places where you really do need more screen real estate.

**Leo:** I have to say, I bought a 30-inch display for my Mac, and which is a single display; but, I mean, it's a lot of real estate. And I'm actually thinking about getting a second one. I mean, it's funny how your needs expand to fill the real estate you have.

**Steve:** Exactly.

**Leo:** Right now I have a 30-inch and then a 24 - the Windows machine is on a 24-inch to the right of it. And I use Synergy, so I can use one mouse and keyboard with the two computers and two displays. And that works quite well. Synergy's a really neat little program for Windows and Mac. And I just slide the mouse over. So in a way it's kind of like an extended desktop except it's two different operating systems. That's kind of nice, yeah. Yeah, I'm thinking. You've got me thinking. Maybe I need a 30, a second 30. They're so hideously expensive, though. You have - how big are the monitors in front of you?

**Steve:** I've got SGI monitors that I've owned for years. They're 1600x1024. And I've got my next machine set up already. I'm going to be switching to DVI. These are - they're, like, custom cards. They were 3D Labs cards running on these SGI monitors. And at the time they were available for a great price. And I'm not gaming or anything on them, I'm just sitting here looking at text and editing and things most of the time. So I don't need any ultra high performance. But the machine I'll be moving to, I've referred to it before, it's that quad core Intel that I call Quadmire. And it's got, okay, it'll be running Windows. That'll be my move to XP. And I've got beautiful 1600x1200 Dell monitors lined up for that one. I just haven't had any time to make the switch.

**Leo:** Those Dell monitors are really nice.

**Steve:** Oh, they really are. I think I own maybe 15 of them.

**Leo:** Yeah. I have a few. I have a few, yeah. Let's see. Peter Brischetto in Sydney,

Australia wants more discussion of enterprise security: Hi, Steve. I was excited to read the title of the last Security Now! podcast, thinking you'd delve deep into the problem of corporate security and discuss it for hours and hours on end. Well, we just got started, give us a break. Alas, it wasn't to be. I would like to share my experiences with you so that you could share it with your listeners.

At my previous employer, I was the network administrator for a software development firm with about 40 staff. Every developer had a company-provided laptop that not only had XP on it, but also required them to run IIS, the Microsoft SQL database, Visual Studio, and other such applications. Being laptops, they were often connected to third-party networks like client networks, hotels, even their own home networks. To further complicate matters, while in the middle of a development cycle, many of the developers would refuse to install Microsoft's many updates - I don't blame them - updates, patches, service packs to any of their software as this had caused their development environment to break. As you can imagine, I didn't have much confidence in the security of our network.

The solution we came up with worked great for me, the administrator, and also for the developers. We implemented VMware on all developer laptops. A VMware image was created for each client that the developers would then use on their laptop for the purpose of development and testing. This allowed their native Windows XP install on their laptop to be kept fully patched without also having to run SQL, IIS, and other problematic software on the outer machine. The VMware image was limited in its network connections, and regular snapshots were taken so if the image went bad it could be wiped and rolled back to the previous snapshot. The added benefit to the developers is that when a new developer came onto a project, they could be up and running with the latest VMware image in minutes.

I've since left this company and now work as an IT consultant for small businesses. This is more of a challenge, as I'm not only telling businesses what they can and can't do with their computers, but the experience and requirement level differs greatly from business to business. I'd love to hear other network admins' experiences with their IT security and the problems they face. Love the podcast, and of course SpinRite.

**Steve:** Well, I thought that was a very clever solution that Peter came up with.

**Leo:** Yes.

**Steve:** We've of course talked about virtual machines and the isolation that they provide. And there were a number of people who sort of expressed similar sentiments of really, really being captivated by the topic of enterprise - and the challenge of enterprise security. So I wanted to have you share Peter's experience, but also to invite anyone who has their own stories like this - solutions, problems, dilemmas, that kind of stuff - to drop a line to us. It's GRC.com/feedback is the page where people can submit things. Make sure you put something in the subject line, like say "corporate security" or "enterprise security," that'll catch my eye. And we'll try to give that some more time because I really think certainly it's an interesting different sort of set of problems, just due to the nature of network and uncontrollable users and telecommuters and all that. So it's enough different from certainly the related topics that we typically discuss, I wanted to give it some additional time.

**Leo:** Yeah, we've never not done enterprise, but we've never specifically done it. I think everything we talk about is applicable really to a wide range of computing. Obviously a lot of IT pros listen.

**Steve:** Exactly.

**Leo:** And I hesitate to just say this, you know, we're going to focus only on enterprise, because that would leave a lot of the audience out, as well.

**Steve:** Exactly. And certainly we're not going to do that. But we just - we would never - well, I guess my point is that solutions like what Peter talked about...

**Leo:** That was great.

**Steve:** ...have all kinds of applications.

**Leo:** Yeah. That's useful across the board. We talk about high-end computing. I think if you were to say what it is, it's high-end computing, which is applicable in a variety of situations, including the enterprise. TWiT has never done much enterprise stuff because I've just never been that interested in it. I've always been end-user focused. Higher, higher end user, and high enthusiastic focused.

**Steve:** And we know that's where I come from, too.

**Leo:** Yeah, yeah. And, you know, even though this - it looks like a business, and we have advertising and so forth, we really do it for fun, too. We want to cover the topics we're the most interested in. I'm sure there are many enterprise security podcasts out there you can listen to. Of course, none of them have Steve.

Javier Gordo of Katy, Texas wants sticky windows. Oh, yeah. Steve, you mentioned some time in the past a small app that would make Windows' windows edges sticky, so that they'd lock to the edges of the screen and to each other. I changed computers. I can't find the name of the app. I miss it, and I've got to have it back. What's it called?

**Steve:** Well, I loved this because I totally understand that sentiment. The program is called allSnap. And we've got a link to it in our show notes for this Episode #128. But it's also just www.allsnap.org is the site. It's a tiny little tool. I have it running on every single one of my Windows machines. And when I, I mean, I almost want to, like, bring it with me if I'm forced to touch anybody else's Windows machine. I mean, I just, it's - I don't know, Leo. We've joked about it in the past. I used to sit there, literally spending time trying to get my window edges lined up with the edge of the screen, just because I didn't want any - I didn't want it to go too far, I didn't want to see any background coming through, I like everything sort of positioned right. And allSnap just, well, makes it a snap.

And it's funny, when I was doing a little digging around I ran across another piece of freeware that appealed to somebody who was also an allSnap addict. It's called Taskbar Shuffle. And it's now running on my machine. It's very simple also. It simply allows you to shuffle, that is, reorder your taskbar button. It's funny because I have some things that start up at the very beginning when I boot Windows. So they're naturally over on the left side of my taskbar. And I sort of get used to them being there, like my email client will be over there. But when I shut my email client down, and then later - as I have, for example, during the podcast - and later start it up, well, now it comes up over on the right, where newer apps are. And it sort of bugs me because I'm used to it being over there. Well, with taskbar shuffle you just, literally, you just click on the button, drag it over where you want it, and you're able to put them in any

order. It's like, and I have to say, I wished I had that for many years. Now I do. So there's also a link to Taskbar Shuffle in the show notes. And if you just put Taskbar Shuffle into Google, it'll take you right to it.

**Leo:** Taskbar Shuffle.

**Steve:** Oh, and you can also, if you care, reorder the little icons in your tray. You hold Ctrl down. You can grab the icons and move them around. I'm less concerned about their order than I am my main Windows taskbar icons. But anyway, now everyone knows about, or knows again about allSnap, which I love, and about this new little gizmo, Taskbar Shuffle.

**Leo:** It's good stuff. Leo in New Jersey - I like that name - wants to keep control of his machines: Hi, Steve, my name is Leo. Somebody just tuning in is very confused right now. I'm 16 years old, and I'm the resident IT guy everybody goes to for advice. My question is this: I have a downstairs computer I use as a torrent box, mom, dad, houseguest computer.

**Steve:** Sort of a throwaway machine.

**Leo:** Yeah, let Mom and Dad use the torrent box. Would Windows SteadyState work for me? Oh, SteadyState, that's what we were talking about the other day. I have my admin account as my torrent area, my limited account for Mom and Dad - Leo, you know how to treat your parents. If I wanted to make a SteadyState account for my parents and another one for my houseguests, would that work? Will I still be able to keep my admin account? So let's say I have to add software to the whole machine, or update AV definitions, not just my account, how do I do that? When I install software in the admin account, does it then go to the SteadyState accounts? Also AV scanning, do I need to scan with an AV if I'm using SteadyState? What, what, how does it work?

**Steve:** Well, we've never really needed an inter-episode teaser...

**Leo:** But that was it.

**Steve:** ...but that's what this is. Because Windows SteadyState is the topic of next week's Security Now! podcast.

**Leo:** Cool.

**Steve:** So if Leo can hang in there for one week, we're going to answer all of those questions and talk in detail about it. I've been working with SteadyState now for - I've been going steady with it for about four weeks. I am very impressed. I'm going to be recommending its use in all sorts of environments. It really solves a bunch of problems. And it would be a perfect solution for Leo to essentially control what his mom and dad and his houseguests do with that computer when it's not under control of Torrent.

**Leo:** So just quickly, do you want to just kind of thumbnail what SteadyState does? I think

we mentioned it last episode, but just so people know what we're talking about?

**Steve:** Yes. It is a free facility that is now being offered by Microsoft. It was known in a sort of an unpolished prior version as, like, Shared Access Toolkit for Windows, something, I don't remember the exact name, but it was like that. It has been matured and packaged into a single, simple, easy download. And essentially it has some characteristics of System Restore, where you're able, for example, as we know with System Restore, to back up if something bad happens to your machine. But it is way more bulletproof. It allows you to really lock down a system.

Its typical use is - and again, it's sort of hailing from the Shared Access area - would be, for example, a Windows machine running XP. It needs to be XP. Vista has this technology in some flavor built into it. So this is not something for Vista. This is specifically for Windows XP. Nor will it run on Windows 2000. It needs the features of XP. But if you ever had a machine that you need to, sort of by nature, expose to a hostile environment - like for example in an elementary school, where you've got a lab of machines that you want to allow students to use, or in a public library where, again, you want to make some machines available for doing Internet research, yet lord knows what the computer users are going to do to them - this is a way of constraining what they can do, and at the same time protecting the machine from them.

My particular focus was in a corporate environment, which is the reason I really got focused on this, is would it be possible to allow the selective preservation of things, like the contents of a user's My Documents directory, which is not the default configuration. But I worked all that out, and that's what we'll be talking about, in addition to many other things, next week.

**Leo:** Goody goody, I can't wait to find out. Well, you'll want to tune in Episode 129. Our next thrilling, gripping edition of Security Now! will be on January 31st. And meanwhile, Steve, have a great week. And we'll see you then.

**Steve:** Perfect.