Listener Feedback Q&A #34

Description: Steve and Leo discuss the week's major security events and discuss questions and comments from listeners of 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 we have previously discussed.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-130.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-130-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 and Leo Laporte, Episode 130 for February 7, 2008: Listener Feedback #34. This show and the entire TWiT broadcast network is brought to you by donations from listeners like you. Thanks.

It's time for Security Now!, ladies and gentlemen, and I'm so glad to see Mr. Steve Gibson on the other side of the microphone. Hello, Steve.

Steve Gibson: Hey, Leo, great to be back with you once again. Episode 130, 130.

Leo: 130, it's amazing. Separated only by the state of California. I'm in the north, you're in the south. And so actually, if I were to see you across the microphone, it'd be very dim and tiny.

Steve: Yeah, well, you would have exceedingly good eyesight. Actually, I think the curvature of the Earth would completely preclude that.

Leo: I think you're right. You're a scientist at heart, and you can't get away with any of this fantasy stuff with you. No, I'm just finishing - not finishing. I'm really in the middle of "Nights Dawn Trilogy." Actually, you can't finish it. It's the world's longest book. The "Night's Dawn Trilogy," Peter Hamilton, really great.

Steve: Oh, are you loving it?

Leo: Yeah, well, it took a little while to get into. I couldn't - because there's so many storylines in it.

Steve: Yes.

Leo: And they're very diverse storylines, you know. So it took me a little while to kind of start piecing it together. But that's part of its charm because once you do - I don't know how many pages in I am because the Kindle only gives you paragraph markings. But once you get a little far in on it - I'm three dots in, three or four dots in. And...

Steve: Oh, and you probably have, like, 20 dots to go.

Leo: Oh, it's a big book.

Steve: Yeah, yeah. And it...

Leo: Well, the Kindle always has the same number of dots. Have you noticed that?

Steve: Yes, although the, I mean, it is a proportional...

Leo: Right.

Steve: It is a proportional display, so...

Leo: Right. Hey, there's some cool Kindle hacks. I know, I think you mentioned this the other day; but do you know about the one that, where you turn the radio on and then go to the Kindle browser, if you press Alt-1, it'll open up the Google Maps at your location?

Steve: No.

Leo: Yes. Yes.

Steve: Very cool.

Leo: Because the cell - well, at your location. It's the nearest cell site.

Steve: The only thing I really want is an onscreen clock.

Leo: Okay. That's one of the hacks.

Steve: Yay.

Leo: I'll tell you - I'll look it up, and I'll tell you before - because I don't have it right in front of me. But there is a simple keystroke that will put a clock on the screen at the bottom of the menu.

Steve: Oh, no kidding.

Leo: Yeah.

Steve: So it's already built in there somewhere, it's just hidden.

Leo: Exactly. There are a - you know, the Kindle actually had a bunch of, a surprisingly large number of undocumented keystrokes.

Steve: Well, it's impossible to ever surprise you about anything going on in the industry. But I had a note here to mention to you that Amazon is buying Audible.

Leo: Yeah. Yeah, that didn't surprise, I mean, that surprised me. But, yeah, we've known about that for a little while. And actually Audible is now a sponsor of this show, as well. Happy to have them onboard. They're on every show.

Steve: You mean Security Now!?

Leo: Security Now!.

Steve: Oh, no kidding.

Leo: They're on every show on the TWiT network. They're a big - in fact, the day before the announcement, I got a very nice email saying how happy they were, how they looked forward to 2008 and a great relationship, and they were going to renew this through the rest of the year. And then the next day Amazon bought them. Now, I don't know if that's, you know, how that's going to affect anything. So...

Steve: Right.

Leo: But nevertheless, it was, you know, yeah, a little bit of a surprise. So the guy you'd be interested in who hacked the Kindle - actually, I'd love to get Amazon as a sponsor. Goodness knows, Kindle should be advertising on this show.

Steve: Have you see the count on my review on Amazon's site?

Leo: How many?

Steve: It's, like, 11,000, I think. It's way more than twice the #2 review, so.

Leo: Well, you'd like this Kindle hack because the guy who did it, I'm still Googling around to try to find - oh, it's Igorsk. The guy who did it, this is - he got the ROM code, disassembled it, and figured it out.

Steve: Oh, beautiful. So pure reverse engineering.

Leo: Yeah. I mean, beautifully, beautifully done. It's just really remarkable. He starts by figuring out how to get root on it. And then he is able to download the code, disassemble it, and that's how he finds all these undocumented keyboard shortcuts. So let me find the time one. There's Minesweeper in it, by the way. Did you know that?

Steve: You know, I may have run across this article because I remember seeing...

Leo: You talked about it, I think...

Steve: Yeah, I remember seeing a whole list of goodies. But I did not - it didn't click with me that a clock was among them. So maybe there's a newer list.

Leo: So Alt - okay, there's a couple. In the reader, at home, Alt-t shows the time. Do you have your Kindle in front of you?

Steve: No, I don't have it in front of me.

Leo: Okay, this is so very funny. Well, I won't tell you what happens. When you're reading, do an Alt-t. Oh, I'm going to tell you.

Steve: Okay.

Leo: It doesn't show the time digitally. It spells it out. It says, like, half-past six. Because you're reading. So I thought that was funny. Alt-t, that's what you need to remember.

Steve: So the people who did this clearly had some fun.

Leo: Igorsk. Igorsk did it. And...

Steve: No, no, I mean the Amazon guys.

Leo: Oh, there's tons of stuff in there. Oh, yeah. And it wasn't at Amazon. It was Lab126. So if you go into settings and enter some numbers, you can see the Lab126 team members if you enter 126. They clearly did. There's a lot of stuff in there that is kind of not documented. So anyway, I just thought I'd pass that along.

Steve: That's very cool.

Leo: We have also Astaro back with us, so I'm going to do an Astaro commercial in a little bit. But do you have, before we do that, do we have any addenda? Oh, and we should tell people, this is a Q&A episode.

Steve: Yup, Q&A episode. I've got all kinds of stuff. I did want to mention that Yahoo! joins the ranks of being an OpenID authentication provider.

Leo: Yes. Isn't that great news?

Steve: Yup. So they're now supporting OpenID, which I hope will do a lot to promote OpenID. Unfortunately, they're only a single-factor authenticator. So, you know, they're not competing with VeriSign's VIP. And in fact it'd be very cool if they were to add that to VeriSign. So if we've got Yahoo! members who would consider using Yahoo! as an OpenID provider, you might drop Yahoo! a little note through their support link and say, hey, how about adding VIP authentication because it's going to be even more secure that way, as we all know.

Leo: Of course we all know, if Microsoft buys them, then who knows.

Steve: Yeah, I was wondering about that, too, so.

Leo: I mean, I'm actually a little disappoint- I hope that doesn't go through because I think - I like Yahoo!, and I like their range of services, and I like their support for things like open source and OpenID. And of course all that would change if they were a Microsoft company.

Steve: Yeah, well, we've got, you know, hungry Ballmer is out scouting around, trying to get them, so...

Leo: He's trying to beat Google, is what he's trying to do.

Steve: Let's hope not, yeah.

Leo: Also I have a couple of addenda when you're done.

Steve: Yeah.

Leo: Just to let you know.

Steve: Okay. Well, I've got - I did want to mention that I'm loving Jungle Disk. It just updated itself, or told me that there was one. It's up to 1.50c, and he's been fixing little things here and there. So, I mean, I'm just - I got my bill from Amazon for last month? 10 cents.

Leo: I know. I got 3 cents.

Steve: And I have a ton of stuff up there. And, I mean, I just love it because I can - if there's something that I absolutely want to have universal access to, like I'll drop some - I just sent - I sent 120MB up there because I don't have my laptop with me. But when I do next, I'll want to be able to yank that thing down from Amazon. So it's just sort of, you know, it's data storage in the sky, and it's not very expensive.

Leo: And Jungle Disk makes it look - it's WebDAV, right, so it makes it look like a mounted disk.

Steve: Yes. Under XP and Vista, the WebDAV client is built in. So you're able just to map it to a drive. I'm still using Windows 2000. I did find a - I found a product that allows, that essentially adds that feature to Windows 2000, although there is the ability right now just to browse to that sort of like a folder, where you don't have a drive mapping. And I find that's just as convenient as having it as a drive letter. It wouldn't be, however, if I needed to, like, automate things, like use my own backup solution rather than the one that's built into Jungle Disk in order to do that, so.

Leo: Yeah. Because looking for a drive letter is so much easier. Every program can do that.

Steve: Well, I've got two really fun security event stories. This one's just going to boggle people's minds. It's funny, years ago, many, many years ago, I remember refusing to talk to my attorney on my analog cell phone at the time because I knew that it wasn't secure. And that was probably my - and I remember him thinking, c'mon, Steve. I said no, no, no, no, I'm in the car right now. I'll call you back when I get to the office because this is a radio, and I'm not having a conversation with my attorney on an analog cell phone. And so he's like, okay, fine, well, call me back.

Leo: And you were right, by the way. I've talked to many guys, many hackers who just kind of made a habit of listening into analog cell phone recording...

Steve: Oh, some, I mean, you could have some fascinating things that you would overhear. And so it's like, radio, I mean, I know that listeners of Security Now! know how skeptical I've always been about radio. Well, this story that just surfaced just really drives this home. This was written, this was posted on DarkReading.com by Steve - I'm going to wreck his name. But I'm not - I'm sorry, Steve, I'm trying not to. It's Stasiukonis, something, Stasiukonis, something. Anyway, he's a VP and founder of Secure Network Technologies. They are a security penetration testing firm. Okay, now, this is a true story. And it's got a serious theme to it because there's one other area of wireless that is still - people are not thinking about it.

Anyway, he says, in offices all over the world, users are becoming increasingly enamored with those wireless, hands-free headsets that allow the speaker to move around the office while continuing a conversation on the phone.

Leo: You're not talking cell phone headsets. These are for land lines.

Steve: Exactly. So instead of having the coiled cord where you're having to stretch that around, you replace it with a little base station and wireless headset. And he says, have you ever wondered how secure those headsets are? So have we. Recently we had the chance to find out. And what we discovered was downright scary. If you don't know us, Secure Network Technologies is a penetration testing firm that focuses closely on the issues of physical security and social engineering. We were recently hired - okay, so they were hired, so what I'm about to describe here is legal. They were hired by a large organization to assess the company's network security and other potential vulnerabilities. Always anxious to try new things, we asked to test wireless signals leaving their building, including wireless access points, radio frequencies, et cetera, and potential vulnerabilities in those hot little hands-free headsets.

To perform the work, we purchased a commercially available radio scanner. These devices are available at any local electronics retailer at prices ranging from $80 to several thousand dollars. We chose a scanner capable of monitoring frequencies from 900 to 928MHz and the 1.2GHz ranges, which is where many of the popular hands-free headsets operate. We took a position across the street from the facility and started up the scanner. Within seconds of turning on the device, we were able to listen to conversations that appeared to be coming from our client's employees. Several of these conversations discussed the business in detail, as well as very sensitive topics.

After some careful listening, we determined that the conversations were indeed coming from our customer. After confirming that the source of the conversations were on our client's premises, we made note of the specific frequencies that were used and locked in on them. We could then record the conversations digitally using the scanner. Within minutes of this discovery, we contacted our customer and explained the vulnerability. We felt this issue could not wait for our final report. To demonstrate the sensitivity of what we discovered, we used the conversations we recorded to social engineer our way into the facility.

Leo: Oh, boy.

Steve: We gathered the names of people mentioned during conference calls, as well as other specifics about each person. We then singled out people that were foreign to the location we planned to enter. We singled out the names of people whom the callers had never met, people who had never been to the location, and people who were new to the organization. Our plan was to assume an identity of an employee who had never been to the office we were testing. Using that identity, we would enter the building, commandeer a place to sit and work, then see how long we could stay inside the building. After zeroing in on a particular employee, we gathered as much intelligence on him as we could. To prepare for the entry into the facility, we printed a business card with our assumed identity. I put on my best suit...

Leo: This guy likes his work way too much.

Steve: Oh. I put on my best suit, he says, and then went to work. When I entered the building, I was greeted by security. I indicated I was an employee and was in town to work. I handed the security guard a business card and was welcomed with a smile. After escorting me to a cubicle,

the guard showed me where the restroom was, where I could get a cup of coffee, and how to go about getting a building access card. After settling into my new workspace, I plugged my laptop into the network, started my network scanning tool, and retreated to the cafeteria for lunch. Upon my return I was presented with a card access key to the building. The card was accompanied by a document outlining security policies regarding its usage. Clearly the people who issued it never checked deeper into who I really was.

With access card in hand, I started exploring the building. I had almost complete access. In the few places where the card did not work, such as the server room and fitness center, I used additional social engineering tactics to gain access to those, as well. By day two I was already accepted as an employee. In the morning I greeted - I was greeted by my would-be coworkers and security folks. I began to take some liberties such as booking conference rooms, asking for refreshments, and gaining permission to bring in a "vendor," unquote, actually Doug Shields, my partner here at Secure Network. In all, I spent three days inside the building, gaining access to numerous types of information, resources, and technology.

Leo: Oh, my goodness.

Steve: Our social engineering effort was just one exploit. The real danger is the information that was being emitted across the street from the company through the wireless headsets. This technology is convenient, but it is opening companies to potential calamity. With the data we heard, we could have made a stock play, provided valuable information to a competitor, or gone to the press with scandalous data. We also noted that when conversations ended, the headsets became bugging devices. Even after calls were terminated we could hear headset-wearers breathing, as well as any other conversations that were going on in their offices.

Leo: Oh, my goodness.

Steve: We were interested in this vulnerability, so we asked for permission from other clients to test it out at their locations, as well. We ended up intercepting communications ranging from financial institutions, healthcare, and a variety of other professions and industries. We heard conversations from administrators of computer networks, C-level - that is to say CEO, CIO and so forth - C-level executives, legal departments, and management teams. What did we prove? That many companies which fear security breaches and eavesdropping are actually bugging their own offices and spilling their private content over the open airwaves without their knowledge.

Leo: Unbelievable.

Steve: The problem is not unlike the early days of wireless LANs and WiFi when the technology became popular before adequate security was developed. What can you do about it? The first step is to recognize the vulnerability. These headsets generally operate at 900MHz and, as we learned, are not necessarily secured with encryption. Find out who's using the technology and where. Secondly, you should consider doing a scanning test of your own, as we did for our client. It's worth 80 bucks to make sure your corporate secrets are not unintentionally leaking out of the building via wireless headsets.

Leo: Now, just to make it clear, these wireless headsets aren't the same as, say, a cordless phone, or are they?

Steve: No. These are add-ons to typical corporate phones. I mean, I've got one around here somewhere.

Leo: Oh, yeah, I have a Plantronics right here, I'm looking at it.

Steve: Yes, very much like that. And they are simply trans- I mean, this is exactly like me refusing to talk to my attorney on an early analog cell phone. I mean, arguably that was even worse because there you've got serious range. But these things work across the street. And, I mean, in this case this guy, simply by overhearing conversations, was able to function as an employee in a company where he wasn't employed. The higher ups knew and gave him permission to do this. But that permission was entirely optional. I mean, anyone could do what this, you know, Steve and his partner, was it Doug or David, were able to do.

Leo: That's just amazing.

Steve: So I just wanted, I mean, this report, I just read this, I thought, okay, we've got to talk about this. I mean, just the idea that these little - they're basically handset extensions. And, you know, people who use them are bugging themselves.

Leo: Yeah, wow.

Steve: Okay. Second amazing story of the week.

Leo: Okay.

Steve: This is also frightening. I mean, this is - what I'm about to read is horrifying and true. It was posted by a blog at Symantec, describing an amazing trojan known as Silent Banker. What's really fun about this, too, is that - I'm going to read the blog entry. It touches on so many things that we have already talked about. So, I mean, this is a little bit of a walk in the park for our listeners. But the blog entry was titled "Banking in Silence."

Targeting over 400 banks, including my own, writes this blogger, this Symantec blogger, and having the ability to circumvent two-factor authentication, are just two of the features that push the Silent Banker trojan into the limelight. The scale and sophistication of this emerging banking trojan is worrying, even for someone who sees banking trojans on a daily basis. This trojan downloads a configuration file that contains the domain names of over 400 banks. Not only are the usual large American banks targeted, but banks in many other countries are also targeted, including France, Spain, Ireland, the U.K., Finland, Turkey, and the list goes on.

The ability of this trojan to perform man-in-the-middle attacks on valid transactions is what is most worrying. The trojan can intercept transactions that require two-factor authentication. It can then silently change the user-entered destination bank account details to the attacker's account details instead. Of course the trojan ensures that the user does not notice this change by presenting the user with the details they expect to see while all the time sending the bank the attacker's details instead. Since the user doesn't notice anything wrong with the transaction, they will enter the second authentication password, in effect handing over their money to the attackers. The trojan intercepts all of this traffic before it is encrypted. So even if the transaction takes place over SSL, and of course we know we certainly hope it would, the attack is still valid.

Unfortunately, we were unable to reproduce exactly such a transaction in the lab. However, through analysis of the trojan's code, it can be seen that this feature is available to the attackers. The trojan does not use this attack vector for all banks, however. It only uses this route when an easier route is not available. If a transaction can occur at the targeted bank using just a username and password, then the trojan will take that information. If a certificate is also required, the trojan can steal that, too. If cookies are required, the trojan steals those, as well. In fact, even if the attacker is missing a piece of information to conduct a transaction, extra HTML is added to the page to ask the user for that additional information.

And he shows two screenshots here. I made a shortcut for this blog entry because it's really worth looking at for our listeners. It's just SnipURL.com/sn130. That's the episode number of Security Now!. So anyone can put SnipURL.com/sn130, and they'll get this blog posting.

He goes on to say, when instructed, the trojan can also redirect users to an attacked-controlled server instead of the real bank in order to perform a classic man-in-the-middle attack. Currently there's only one bank targeted in this way. However, recent updates to the trojan - oh, and get this. It gets constant updates using updated software. He says...

> **Leo:** If it's working, why not?

Steve: Yes. Recent updates to the trojan change the user's DNS settings, which we were talking about just recently a couple weeks ago, change the user's DNS settings to point to an attacker-controlled DNS server. Using this technique, the trojan can start redirecting any site to an attacker's site at any time. This feature could also mean that, if the trojan is removed, but the DNS settings are left unchanged, then the user will still be at risk. See below for the attackers' DNS server addresses.

Add to all of the above the ability to steal FTP, POP, webmail, protected storage, and cached passwords, and then we start to see the capabilities of this trojan. But it doesn't stop there. Don't forget the porn. The trojan also contains over 600 pornographic website URLs that can be shown to the Internet user so that the attacker can make money from the referrals. Lastly, the trojan can also download updates, which it regularly does. It can also upload other executables and can use the infected image as a proxy or as a web server on any chosen port. In tests, the HTTP port used was 18102. The multiple configuration files that the trojan downloads are updated several times per day, so it's more current than Windows is.

> **Leo:** More current than anything.

Steve: Yeah.

> **Leo:** More current than Norton Antivirus.

Steve: And currently the trojan is capable of injecting HTML into about 200 different URLs, meaning that, as a web page is being displayed by the user's browser - and this thing knows about both Internet Explorer and Firefox - as the web page is being displayed, the trojan is able to intercept that communication and insert its own modifications, its own HTML, into the page. He says, the configuration files are compressed and encrypted. However, after decrypting them we can see how the trojan works in detail. And then he goes on into some additional details, which many of our listeners may find interesting.

Anyway, I mean, this is a beautiful posting because it gives you a sense for just how

sophisticated trojan technology is becoming. And, I mean, how much effort people are willing to go to for this kind of high-value attack.

Leo: Well, it also introduced to me a new category. I never heard the phrase "banking trojan." But obviously these are trojans aimed at corrupting your Internet banking experience; right?

Steve: Exactly. So you're right. There is now a classification of trojans, a set of trojans, of which this is perhaps - and this guy, from everything he's seen - is the most sophisticated one of all. And for, well, for one reason. It's not like it's one trojan for one particular bank. And so you're - how many - what's the chance that the infected user is going to...

Leo: 400 banks.

Steve: Yes. And it's got specific scripting technology in order to deal with each one on a bank-by-bank basis.

Leo: So just to understand, it would get on your computer as an end-user, and it would intercept information about your banking login, basically.

Steve: Correct. Essentially you really don't want this trojan on your machine if you're someone who does online banking.

Leo: And he mentions it's all over the world. I mean, it's not just U.S. banks, it's banks all over the world.

Steve: Right.

Leo: Wow. So, something to be aware of. You know, banks, I think, routinely cover up these kinds of losses. But this is a loss to you. This wouldn't be a loss to the bank, exactly.

Steve: Right. Exactly. You might very well go to check your balance and find that it has been zeroed. Because this thing watched you log in once. And, I mean, might right then have executed a funds transfer. If not, it knows how to - it's able to send this back to headquarters, and then somebody else can log in as you, even if, as this thing, I mean, this thing is so comprehensive that whatever authentication data is necessary - it understands, for example, you know, grabbing cookie details. So somebody could literally pretend to be you, even if you had static cookies on your machine to identify you. And, for example, we've talked about how authentication strength is reduced in instances where you do have a cookie because you've already authenticated your machine to the bank once before. And so it says, oh, well, you know, here's a cookie we recognize. We'll only ask for the username and password and not, you know, which kitten the guy, you know, has chosen in the past.

Leo: Right, right. Hey, I had a couple of emails I wanted to just fill you in on. One is from - actually I got it from a number of people. But Rami was the first, he's a level designer at Ubisoft Montreal. Deep Freeze was the name of the program I was trying to remember. We

were talking about Windows and Microsoft's capability of, what was the name of the Windows...

Steve: SteadyState.

Leo: SteadyState. So Deep Freeze is from Faronics. And I've had a number of people recommend it to me in the past, does something very similar. It kind of resets the machine on every reboot.

Steve: Is it free?

Leo: No, it's not. And Microsoft's is. But Deep Freeze isn't hugely expensive. It depends on how many seats you have and so forth. It's 45 bucks just for the basic...

Steve: Oh, okay.

Leo: So it's not hugely expensive. But if you had hundreds of seats it would get more expensive. And then I want to thank Randal Schwartz and many other folks who are fans of TrueCrypt. The good news, you probably heard this also, there is now an OS X TrueCrypt. Right when we started talking about it, I went to the TrueCrypt site, and it said we're working on a Mac beta. TrueCrypt 5 is out and in fact works on OS X. I've downloaded it. In fact it is compatible across OS X, Windows, and Linux. So you can have a TrueCrypt-encrypted file, folder, or disk, and you could read it on any of those three operating systems, which is...

Steve: Very cool.

Leo: Yeah.

Steve: And in fact there was so much interest in this that our Q&A that we'll be getting to shortly talks about some things that are built in already to the Mac.

Leo: Oh, yes, of course. And now it's time. Are you ready?

Steve: I'm ready, Leo.

Leo: You feel good? It's question time. And we'll start off with Lin in Kalamazoo. Lin has a lot to say: Hello, Steve and Leo. Longtime listener here, started off with you on show 01. Should that have been show 00? Yes, in true programmer's form I should have named it 00. TWiT started with 00. But I don't know why, I just - I wasn't thinking. We started with show 01.

Love the show. Frequently relisten to past episodes to keep your ideas and teaching fresh in my mind. We do recommend that. [Indiscernible] gain anything from that, but I think

there's an advantage to that, you know? Listen again and again. I don't gain anything from it, Steve. You know, it's just I like that idea. I have to listen to it again. I get something more every time.

I'm on the road about three hours a day, so I get a lot of Security Now!, and I love it. Additionally, about six months ago I became a SpinRite customer. I have 11 computers, 30 hard drives at home. What? Like most of your other listeners, I've saved several drives and many gigabytes of information with SpinRite. I don't know how I lived without it. Your last episode reminded me that I, too, had a few old broken dead drives in storage. Remember we were talking about that, you know, somebody had resurrected a drive they hadn't used in, what, they had wrapped it up and hadn't used it in years.

Steve: Yeah.

Leo: So it's kind of like cutting off your head and hoping that - and freezing it. Someday they'll be able to resurrect you. So I was able to revive them and get some cool data I'd missed over the years. You know, I have to do that. I have tons of drives. Everybody does. Just, you know, old 20MB drives, things like that. It would work with any drive; right?

Steve: Sure, any IDE drive. And, I mean, even pre-IDE if you still have the controller lying around.

Leo: MFM, RLL, remember those?

Steve: Yup.

Leo: Your last episode - oh, yeah, okay. My longest drive recovery - oh, get this. Now, our record is three months, I think; right?

Steve: I think so.

Leo: He took 17 days. That means his SpinRite was running for 17 days, but he's patient. He'd heard about three months, I guess. My SpinRite finally sorted everything out. I was able to get what I needed back from the drive. One question, though, about SpinRite: I have an expensive aviation Garmin GPS unit that's having a memory issue. It has 512MB of RAM it treats as a drive. I can't get DOS to see it as a drive. Or I can get DOS to see it as a drive if I plug it in via USB. Can I get SpinRite to work on it? I'm a pilot, and I really depend on my GPS. I'd love to save the two grand from buying another one. Those are vital, you know, those GPSes. Problem is USB; right?

Steve: Well, and I don't know exactly, he says he has a RAM issue. I would advise him not to use SpinRite on that system because you really don't want to run SpinRite on non-volatile RAM. All it will do is tend to bring it closer to its end of life. So I never recommend running SpinRite on any kind of non-volatile solid-state storage. We've talked about how ultimately all it does it move them further toward end of life. So it's really not what you want to do. I don't know enough about his system, what kind of an issue, as he puts it, he has. I mean, if DOS will see it, SpinRite will run on it.

Leo: It's a little USB drive, though.

Steve: Oh, yeah. Absolutely.

Leo: Oh, it will.

Steve: Yeah.

Leo: I thought the USB interface hid drive essentials that you needed to see.

Steve: No, you can still read and write. And SpinRite's able to back itself off and use as much of the available interface as possible, so...

Leo: So you won't get the low-level stuff.

Steve: Correct, correct. You don't have the ability to talk as intimately to the drive as when you plug it onto the motherboard directly. But it still works, and...

Leo: Oh, I didn't know that. Oh, I didn't know that. I thought we had to connect via IDE. Oh, that's good to know. That's good to know. So worth at least trying.

Steve: So, yeah, I would, I mean...

Leo: If it's really RAM. If it's Flash, don't do it.

Steve: If it's Flash, don't do it.

Leo: It has to be non-volatile, otherwise it'd be useless.

Steve: Yeah, see, I don't understand what data he's got there. I would say pull it all off and just reformat it. I would think maybe just reformatting it out to, you know, cure whatever problem he's got.

Leo: There you go. He has more. He says, now onto my questions regarding enterprise and corporate security. First, is Sprint's wireless data card safe? I use a Verizon EVDO card, like the Sprint one. He says: Am I behind - so I'm curious about this answer, too. Am I behind a NAT router? Do I need a software firewall? I've been running the Sprint card for about a year with no issues, but I was wondering what my exposure is. It's a corporate laptop, sensitive data. I thought we should know. I haven't heard about this on Security Now! yet. It fails the ShieldsUP All Stealth test. It has service ports green except for port 22, which is closed. So I failed ShieldsUP, but everything is blocked. As far as - 22 is SSH; right?

Steve: Yeah.

Leo: As far as a router, my traceroute hops seven times in the 68.*.*.* range before going to wired land network. So there's seven hops within the Sprint network. Is there anything wireless data card users should do to stay secure? How do these differ from my home network protected by my NAT router? Second, I've never - should we answer that first before we go on to spreadsheets?

Steve: Yeah, okay. Now, I don't want to freak everyone out.

Leo: Oh, boy.

Steve: But both...

Leo: I'm freaked out already.

Steve: Both types of cellular technology, both GSM and CDMA, unfortunately use encryption that was - I mean, I can just hear our listeners getting ready for this - was designed by engineers and not by crypto people.

Leo: Just like WEP.

Steve: In their defense, in defense of the cell technology, back when this was first done, it was much more expensive to have processing power than it is now. At least in the case of GSM, it's based on a shift register, I think it's three different shift registers with multiple taps, which is one way of generating pseudorandom data. They've tried, the people doing it tried to keep this as a trade secret, tried to keep it proprietary. Bottom line is it's been cracked.

Leo: Now, you understand first of all this isn't - this is CDMA. And it's EVDO, it's EVDO. It's Sprint.

Steve: Right. Right. Now, exactly. Now, but CDMA has been cracked also. So...

Leo: And I don't know if EVDO really uses CDMA technology. It's on those frequencies, but it might use something else.

Steve: Actually it does. All EVDO is really doing is aggregating a bunch of channels together. And essentially that's where you get all this extra bandwidth...

Leo: Oh, interesting.

Steve: ...is it just pulls a bunch of cell channels together and uses them all in parallel in order to increase its speed.

Leo: How interesting.

Steve: I don't know one way or another for sure whether there's an additional layer of encryption on top of the standard cell technology. And when I - again, as I started saying, I don't want to freak out our listeners. It's not like, you know, CDMA and GSM has been cracked to the degree, for example, that WiFi has been. But there are papers on the 'Net that talk about how this stuff can be cracked. So it's not like there's super-strong, industrial-grade, current state-of-the-art crypto. The problem is, these technologies, these digital cellular technologies are so old, and now so widely deployed, that they can't be updated without obsoleting the entire network. And they're, I mean, they're encrypted to the extent that you have to really, really, really want to crack them in order to get inside them. But it is possible. Has been done.

Leo: I'm reading here that EVDO uses a 42-bit pseudo-noise sequence called a "long code" to scramble the transmissions.

Steve: Right. I mean, and...

Leo: That's not very long.

Steve: No, it's not. And again, it's...

Leo: And then it uses AES.

Steve: On top of it.

Leo: Yeah. Well, wait a minute.

Steve: Okay.

Leo: Now, wait a minute. The long code scrambles transmissions through the standardized cellular authentication and voice-encryption algorithm, which is probably the one that's broken, to generate a 128-bit sub-key called Shared Secret Data, SSD. This key feeds into an AES algorithm to encrypt transmissions.

Steve: Well, that does sound pretty good.

Leo: If it's using AES with a 128-bit key generated by random, by pseudo-noise...

Steve: Yeah, it doesn't sound like it's using any kind of a public key technology. And I don't know where the shared secret comes from. It might be based on the phone number, or maybe it's established ahead of time? Anyway, it is on my list of things to research deeply. So I can, you know, we'll spend an hour here before too long talking in detail about cellular encryption technology because I know lots of people are a little anxious about it.

Leo: Well, the thing that makes me anxious is maybe EVDO is secure, the data's secure. But it sounds like voice transmissions over GSM and CDMA are not.

Steve: Right. They would be relying on that initial level of obfuscation, which you really cannot consider as being encryption.

Leo: Right. You know, it's funny because, when we went from analog to digital cell phones, I remember, as we talked about earlier, analog cell phones, just like analog land lines, were completely, completely monitorable. And I remember asking hackers; and they said, well, we don't know how, but probably you could hack into it.

Steve: Probably.

Leo: Probably you could. We just - and this was very early on. He has another question. This is a - you're right, he has a lot to say. But Lin, we don't mind because you're a pilot, and you're going to fly us safe the next time we go up in the air.

I've never heard the question on Security Now! about Microsoft Excel security. Okay. I often time share Excel spreadsheets with people who I want to be able to use the spreadsheet, but not see my formulas or change anything. As most folks know, if you use sheet protection and a complicated 64-bit password, it can be easily cracked in seconds with freeware out there. Okay. My question would be, is there any way to secure Excel so that it cannot be cracked, and you can keep formulas and data from being changed? I did try to use Open Office's XML formatting with protection, but then of course Microsoft Windows customers or Office customers can't use them. Steve and Leo, please help.

Steve: Yeah, this was an interesting question. I mean, he obviously knows that the built-in password protection that's afforded to Excel, you know, there's lots of freeware around that'll crack that easily. The only thing I could suggest -I don't quite understand what he's hoping to achieve. He wants to allow people to view his spreadsheet but not change it. So the thought that I had was to print it to a PDF file. And then they've got the spreadsheet data, contents, charts, and all that stuff in a non-modifiable form, which is apparently what he wants them to see, but not be able to change. So, you know, that was the one thought that I had. Other than that, I mean, you could use external encryption to encrypt the file very strongly. But then you'd have to give anyone the password in order to decrypt it if they wanted to display it. So I don't think that really solves his problem. The only thing I could think was just move it out of an Excel format into a printed form and, you know, share it that way.

Leo: Yeah, depends how he wants people to use it. If he wants them to be able to enter their own numbers, then I think you're out of luck. I think you have to use whatever Microsoft does, and clearly Microsoft's not doing much.

Steve: Right.

Leo: Chuck in Tennessee suffers from debris. Hey, you wrote a little poem there. How do you deal with all the preinstalled junk when you buy a new machine? I've thought of just buying a new copy of Windows to go with every new machine - that gets expensive, have you purchased Windows off the shelf? - just to get as clean a slate as possible. Is this

obsessive? Also, are there a range of running processes that you'd like Task Manager to be showing?

Steve: You know, this is a great question that comes up, you know, often. And I was sort of talking about it the other day. I was very impressed, frankly, with how clean the most recent two Dell systems that I've seen, a laptop and a desktop, they both had virtually nothing on them that I was unhappy with. I also recently purchased some ThinkPads for my employees. And unfortunately there was a bunch of junk there. And I've seen other machines which, I mean, are just, well, oh my god, HP's current offering.

Leo: Oh, it's the worst.

Steve: Oh, Leo.

Leo: HP's the worst. There's nobody worse.

Steve: Oh. I mean, it's just, well, okay. So I've taken exactly the position that Chuck has, which is the only way to deal with this is just to scrape off the machine and start over. Now, I'm a paid MSDN developer, so I have the right to install, for example, XP...

Leo: You pay them, they don't pay you.

Steve: Oh, yeah, I pay them $2,500...

Leo: He pays a lot.

Steve: ...for this, $2,700 or something for a year.

Leo: But you get a licensed copy of Windows that you can install on as many machines as you want.

Steve: Yeah, I don't know...

Leo: So it's no big deal for you.

Steve: I can't give it away, of course. But so that's not a problem for me. My point is that, both with the recent ThinkPad and with the recent HP, even armed with all the drivers that I can find on their sites, I have been unable to install a clean build, a clean install of Windows and get rid of all the little yellow exclamation points under the Device Manager to make it happy again. On a little HP Pavilion I couldn't - I was never able to get the CD/DVD-ROM working. And I tried the same thing on my ThinkPad. I spent two days trying to start from scratch, install Windows - of course I'm using Drive Snapshot all the time in order to make checkpoints. And I should say, of course, that before I did anything I made a snapshot of the - I mean, before I even booted it the first time I made a snapshot of it so that if my attempt to install clean and build it up failed,

then I could get back to the way it was when it first got taken out of the box.

What I ended up doing with the ThinkPad, on all four of them now, is simply removing stuff. I don't like using Add/Remove Programs in order to remove the annoying stuff. But there really was no choice. And I always sort of feel like, well, there's going to be some debris left. It's not really - is it really removed completely? We've had no trouble with our ThinkPads where we just started with the way it came and then backed out of that back to leaving the things installed that are necessary. And, I mean, in most recent cases I've been unsuccessful in, unfortunately, in installing a clean version of Windows and then getting all the various, you know, basically just the device drivers and additional stuff that I wanted to have there working. So it's a mixed blessing. I would just say don't buy HP, you know, buy Dell.

Leo: There are a couple of things to say about that. And Dell used to...

Steve: They've got get a clue about this, Leo. It is so bad.

Leo: Well, Dell used to. And I think one of the reasons they don't, they have this program where they ask users what they want to change. And they've done a number of things. That's why they brought back XP, that's why they offer Linux, and it's why Dell, which has - I think they've done a very good job of removing the junk. There is a program, actually there was a guy wrote it because he was so frustrated with his HP, called the PC Decrapifier.

Steve: Yes, I've heard of that, too.

Leo: Yeah, it's PCdecrapifier.com. It's free. And it does other things. I mean, it's one thing to uninstall stuff. But it also does things like resets the home and search pages, eliminates unnecessary startup items, takes out things like Google and Yahoo! toolbar. So there's a lot of stuff that I think is, you know, this is a choice. The other thing is many manufacturers - well, maybe not many - some will still sell you a real Windows disk as opposed to a recovery disk. The recovery disk, of course, recovers the crap. But a real Windows disk, you know, with the hologram on it and all that, is just a Windows disk. So if it comes with that, then you're golden.

Steve: I should mention, speaking of installing Windows, that I was poking around Microsoft's MSDN site just the other day. And I noticed with glee that Service Pack 3 for Windows XP is now at release candidate 1.0 state. And it's like, oh, please. No more 95 or 98 updates and rebooting nine times for the updates' updates' updates' updates' updates' updates again.

Leo: Well, not for a few months. And then you'll have to do that again.

Steve: Yeah, it's true.

Leo: And by the way, we should mention that Vista SP1 has now been released. It's not - it won't be pushed out to you till March, probably.

Steve: Who cares?

Leo: Some people care. And we'll talk about it, Paul Thurrott and I will, I'm sure, talk about it Friday on Windows Weekly, as well as SP3 for XP. Yeah, because now that's finally out, which is nice. I mean, I don't know if it makes Vista better. But anyway, it's out. So thank you. That was a good question.

Steve: He did also ask about Task Manager. And there's no easy way to answer the question about running processes. But...

Leo: I can tell you a place to go.

Steve: I will say that every so often I will look at, for example, the processes running on GRC's Win2K box. And I'm just jarred by how few there are.

Leo: Compared to XP, yeah.

Steve: When I set it up, I went through, and I turned off all this nonsense, especially for a server that's just going to sit there, you know, it's not - doesn't need all kinds of wacky stuff running. And that's, you know, sometimes I'll turn things off that then I later need, like I'll turn off the DHCP client because I'm not using dynamic IPs within my own network. I'm in a 10. network, and I assign them all myself. And then I'll take a machine somewhere, and it won't connect. It's like, what the heck. It's, oh, wait a minute, I turned off the DHCP. But again, it's like I really do, I bolt these machines down and reduce the running processes just as a matter of best practices in security. And it boots a lot faster, too.

Leo: Black Viper, who did this most famously for XP and then went offline, yeah, is back. He's back. BlackViper.com. And he does have all of the configuration recommendations and the services you could turn off, and at least explains what they do.

Steve: Isn't that so annoying, too, that Microsoft gives you this one little line. It's like, you know, "Tracks changes to multiple files over the network." It's like, okay, well, do I need that or not?

Leo: Yeah, right. And that's what Black Viper - Black Viper was a gamer. But he, by trial and error, went through all these services to figure out what you could turn off and what you had to leave on. So that's a good source of stuff you can turn off. And then of course you can use Msconfig, but I recommend Autoruns, that's Mark Russinovich's program now from Microsoft, at Sysinternals. Just Google "Autoruns" and "Microsoft," you'll find it.

A listener who didn't leave his name wonders about the dark side. Maybe he wants to be anonymous: Hi, Steve and Leo. Thanks for such a great show. I've learned a lot. You guys have never really talked about cracks, pirated software, the whole WAREZ scene. I knew a guy used to call it WA-REZ scene. It surprises me how many people use serials and cracks without considering the security implications. I don't pirate software at all, for lots of reasons. Many people do. Oh, boy, I'll tell you one thing, those WAREZ sites are a hotbed...

Steve: Oh, Leo.

Leo: ...of security exploits.

Steve: It's true confession time. Not long ago, maybe about two months ago, I was really annoyed with my copy of Eudora, which was in standard form several versions back because it had not been giving me a problem. But I was - and, I mean, I love Eudora, I've been using it forever. I actually own many more registrations because I used to have employees that were all registered Eudora users. And so, I mean, and they wandered off and are no longer using Eudora. And so I thought, okay, well - and I was having a problem because one of the cool things Eudora does is it stores all of the contents of a folder in a single text file, which is just nice. The problem is, it tries to parse that file by just scanning the headers, and sometimes it gets messed up, especially if people are including what looks like email inside of email. Then that really gives is heartburn.

So I thought, okay, I wonder if they've, like, fixed this with newer Eudora. So I went to Eudora.com and immediately was greeted with we're sorry, we're no longer publishing Eudora. Version 7.1 was the last one. You can't have it. I think the sponsored edition, which gives you ads in the UI, that you could still have. And then they say, oh, but don't worry, it's going to be going open source, and it'll be coming out soon. So I investigated that. It turns out that that's really not true. Instead the Mozilla people are putting a Eudora UI onto their email client, their communications client.

So it's like, okay, well, that's not what I want. So I thought, okay, what am I going to do? I mean, I own a whole ton of these licenses. I can't get a 7.1. I'd be happy to purchase it if I could, but they don't sell it anymore. So into the WAREZ sites. Knowing the danger of this, I used what I consider a sacrificial computer. Because, as you said, Leo, it is beyond bad. And I did manage to get this machine deeply, horribly infected, just by trying to poke around and see whether I could find something that would allow me to generate a key for a copy of Eudora that I was hoping would work, which again, I would have been glad to pay for, and in fact I've paid for it many, many more times than I'm using it now. So I think, okay, morally I'm - ethically I'm in the clear. But anyway, that's essentially how I feel about this is, again, you want to do what you feel is the right thing. There are solutions out there. But boy, as you said, Leo, they will, I mean, nothing will hose your system faster than poking around in those dark corners.

Leo: Well, just think about it, I mean, if you run a WAREZ or a crack site - actually, no. Let me put it the other way. Let's say you're one of those people who wants to get exploits, trojan horses, viruses, spyware on other people's machines. You bought one of those kits from the Russian website. You just need a website to put all that malware on. Now, what are you going to put together for a website? Well, you're either going to do porn, or you're going to do cracks and WAREZ. That's going to draw people in. Or serial number sites. And so of course that's where all of these exploits are sitting. Now, we used, you know, occasionally on The Screensavers we would need - we would urgently need to run a program, and we would, I'm ashamed to admit it, figuring that, well, the company would want us to show the program on TV, we would go and get a serial number for that program.

Steve: Sure.

Leo: But I haven't done that in years. And I wouldn't dream of doing it, first of all because it's the wrong, you know, I want to buy my software. But also because that's a sure way to get infected. You know, I mean, do it, if you're going to do something like that, do it on a VMware version of Windows that you then erase.

Steve: Well, and that machine was seriously compromised. It had, I mean, little command dialogue boxes were popping up, and then it was installing servers. And, I mean, it was really - I thought, well, I'm sure glad I didn't just go browsing around these horrible places with my "A" machine, or it would be start-over time.

Leo: No kidding. Yikes. Aaron Skinner in Omaha, Nebraska, he's considering going Steady: So here's my scenario. I am running Windows XP, Media Center Edition 2005. I have a couple of roommates who also use my computer. This computer is also used to play some online games. By the way, games like Battlefield 2142 don't seem to run right unless you install and run from an administrator account. Yeah. And that's true. I'd like to have a setup with my personal login, another login for my roommates and gaming. I want my personal login to have full access to everything, and the roommate/gaming to reset after logoff - well, I think we know the answer to this - so no changes are saved, although this may cause issues with game save data. In addition, I still want my Media Center to fully function, you know, record TV shows even if I'm not logged in, or I'm the only one who can do it. I'm also using Avast, which is an antivirus home version, and want to be sure it gets automatic updates. Basically, I want to limit the roommates from doing damage to my computer while leaving my computer and gaming experience unhindered - continuing to run as admin, I guess. I'm interested if and how SteadyState can be used in my situation. Oh, he heard the SteadyState actually.

Steve: Yeah, so he was wondering if it would apply to him. The only problem that I can see is, first of all, Avast, as I recall, was not one of the few AV systems that SteadyState was aware of. There were several, unfortunately, I mean, McAfee was one, and I don't remember now what they were. But there were only a couple that SteadyState could deliberately interact with. And it certainly does require deliberate interaction and operation in order to deliberately bypass this whole drive prophylactic, essentially, that SteadyState wraps your system partition in, your C drive. So I don't think that SteadyState would work for Avast, as I recall, and that's a problem.

The other problem is that doing something like saving recorded TV shows, you do have this driver sitting there which is journaling changes to the system. And, for example, when the admin, the god of that machine logs off, you get a dialogue that says do you want to retain the changes, do you want to flush the changes. So then you decide what you want to do with what has happened while you as the administrator were logged on. Non-admin users, that is to say, anyone who's not that main administrator account, doesn't have the choice, of course. They would be like the user in the library that flushes their changes off the moment they log off. But that does imply that this Windows journaling thing is going along and is on all the time.

So it feels to me like this is probably not the best solution in this case. I would say setting up some sort of virtual machine for these other people to use would give them containment that makes more sense in this environment because I don't - SteadyState is certainly designed in a shared access mode, but doesn't - I think Aaron's application is pushing it a little too far, and I don't think he'd be happy with the way it works.

Leo: Yeah. Okay. And I guess Deep Freeze would probably have exactly the same issues. I mean, anything would that's going to try to maintain that state.

Amir Katz, listening to us from Kfar Saba, Israel - hello, Amir - needs just a little encryption. Just a little tiny bit of encryption: Hi, Steve. You've dedicated a full Security Now! episode to TrueCrypt. You've mentioned it a few times afterwards - and again today. However, I find I don't need to encrypt a whole partition or even a whole folder, just a few files. And AxCrypt is a simple and effective tool for just such tasks, especially if I don't need on-the-fly encryption. It's open source, GPL license, also has a secure-delete feature,

like SDelete, which we mentioned a couple of episodes ago. Can you comment on its security? I find it extremely easy to use. I'm a loyal Security Now! listener from Episode 1, and a proud SpinRite user.

Steve: Well, it's funny, I had to go back and check to see whether I had ever referred to AxCrypt in earlier episodes. And I haven't. Because it's what I use.

Leo: You're kidding. Oh, that's funny.

Steve: No. Yeah. I mean, I discovered it maybe a couple months ago when I was specifically looking around for a - oh, and it's also free, by the way. It's voluntary support through PayPal and Amazon and a few other things. It is a tremendous little program. It is very lightweight. It is different than - I answered a question like this maybe a few weeks ago. And it was a different program, I'm trying to think of the name now, because it was for a slightly different application. And I'm looking here, and I'm - oh, Omziff. That was the encryption tool I recommended because, specifically because it made no modifications to the system it was run on. It was a completely freestanding executable. By comparison, AxCrypt does integrate itself into Windows, so it's more of an installation. It's not quite as standalone. And, for example, it adds right-click context menu support. So, for example, you could right-click on a file and say "encrypt yourself" to the file. So it's a little heavier duty. But I like it very much. And I've been very impressed with it and the way it operates. And now I'm worried I'm going to get AxCrypt and Omziff confused. But I think AxCrypt is the one which can make a self-decompressing EXE, which is also very cool.

Leo: Oh, that's very handy because you can send it to somebody.

Steve: Yes. And so - exactly. So you turn it in, you turn a whatever, an archive of files, for example, into an EXE where, when you run it, it prompts you for the filename. And it's all AES 256-bit, I mean, it's really, really good security. And as he says, it's open source, GPL'd. And you can even download the source from the AxCrypt site. So I absolutely do recommend it. It's a beautiful little program. I like it a lot.

Leo: Good. Well, thank you, Amir. Good suggestion. Another anonymous listener has a question about IP space: Hi, Steve. I work at a large university which owns a Class B public IP range, for example 65.92.0.1 to 65.92.255.255 (that's not the range, but that's an example), consisting of 60,000-plus possible Internet addresses, if my math is right. I've never been able to get info on how much this costs the university, although I know from my work in the private sector that a single IP can easily cost $5 a month. I don't think you multiply by 60,000, but maybe I'm wrong. Whether the IPs are subsidized or not, it seems like a huge waste of money - somebody must be paying somewhere - and an unnecessary exposure to script kiddies and hackers, when over 90 percent of our users would be equally served with a free private IP range. In other words, having maybe one address for the whole university which you use DHCP to share out. Do other universities do this? Are they all subsidized? And if so, are taxpayers picking up millions of dollars in billing for what seems to be nothing more than an increased risk? I'd love to hear your thoughts on this, particularly if I'm totally wrong.

It's not just universities. I mean, Internet service providers, lots of people buy big blocks. A B class is big.

Steve: He's totally wrong. IPs don't cost anything. Unless you resell them.

Leo: Unless you're reselling them, yeah.

Steve: Exactly. So we've never talked about this, so I thought it was a really great question. Back in the beginning we had 32 bits of IP space. And it didn't used to be that networks could be divided sort of on arbitrary bit boundaries. We have talked about this notion of Class A, Class B, and Class C networks. A C class network having one byte of IP addressing, that is to say, 256 addresses, but you only get - you lose a couple from that network. That's a Class C. A Class B has two bytes of addressing, which is what this listener is talking about here, where then you're going to have 64K possible IP addresses within that network. And then of course a Class A you have three bytes of addressing, so that's 24 bits of address space.

So what happened was that the original 32-bit address space was just sort of chopped up in big pieces. There are some universities, and universities were of course part of the early adopters of the Internet, and so this guy works for a large university, they just got themselves a B class network. So they've got, as he said, they have two bytes of addressing, with the first two bytes are fixed, which essentially is the address of their big B class network. And he's very right that it may well be that the university does not need 65,536 or, you know, less a few, individual IP addresses. But they've got them, and they're not going to let them go.

Leo: So they were given them at the beginning.

Steve: Yes.

Leo: As an EDU or whatever.

Steve: Yes. And for example, you know, Level 3, I think, has all of 4-dot. And BBN was one of the other early adopters.

Leo: They invented the Internet. They could probably have anything they wanted.

Steve: I think they've got, like, 1. or 2. something. I mean...

Leo: That would make sense.

Steve: And so essentially the idea is that all of these, the really main Tier 1 ISPs generally own a huge chunk of IP space. I'm embarrassed to say that I at home have 64 IPs, of which I use one, because I'm behind a NAT router.

Leo: And you get that because you bought server service or something; right?

Steve: No, no, no. It's funky because this actually was due to my great relationship in the old days with Verio, where I did need some space, and I had two 32 IP blocks that were disjoint. And so when I switched over, when Verio sold the T-1 business over to Cogent, they took

Verio's engineers, who I knew really well. And Andy, my old Verio engineer, said how many do you want? And I said, well, Andy, I really don't need that many. Oh, c'mon, take as many as you need. And whereas now, for example, with Level 3, who is now hosting GRC's bandwidth, they were like, prove to us you need more than two. I said, well, what do you mean? No, prove you - so I had to literally fill out a sheet showing how and why. And they called it the "IP Justification Form."

Leo: Oh, my goodness.

Steve: I had to fill out a form because they're not wanting anyone to waste them because they're their precious resource, and nobody who ever gets any IPs...

Leo: Ever gives them back.

Steve: ...ever, ever gives them back.

Leo: Mine, dammit.

Steve: Exactly.

Leo: Now I understand. That's interesting.

Steve: It really is. It's a weird sort of bizarre consequence of the early days of the internet, when people would say, okay, how many Class Bs do you need? They'd just chop them up and, you know, because they weren't valuable then. Now they're just - they're the most precious resource on the planet.

Leo: Well, now, I figure we're done; right? Everybody's got something, and there's nothing left. I mean...

Steve: Do you know that there's still only about 60 percent of the IP space is in use? 40 percent is still just slack. It's people like the university, hoarding the IP space because they don't want to give it back. Even though they may not be using it, and somebody else could. It's like, no no no, this is ours. This is our Class B.

Leo: Well, it makes it easier for the record companies because they say, oh, there's 65.92, we know where that is. That's U of A or whatever it is.

Steve: That's very true. And of course after you've been doing networking long enough you just look...

Leo: You start recognizing those, yeah.

Steve: Yes, you can just see the IPs and go, oh, this is Cox Cable, this is Comcast, this is Roadrunner, blah blah blah. Oh, this is an AOL block.

Leo: When you said 4., I said, well, that's Verizon. So obviously Level 1 has given some to Verizon.

Steve: Exactly.

Leo: Yeah. [Brad] Beyenhof has Mac file security pretty well nailed: I've been listening to Security Now! since Episode 1 - again, another great listener - from the actual time it was released, not by archive-diving. I've been listening since day one, he says. In the most recent listener feedback Episode 128 you had a question about encrypting files and folders on the Mac without using File Vault. Oh, I got a number of people sending me this...

Steve: Oh, Leo, I mean, half of the email that I've received recently were Mac people who were proud - so I wanted to acknowledge everybody who wrote in.

Leo: Thank you, everybody.

Steve: Yes.

Leo: And actually, I mean, I should have mentioned it. I've used this technique for years. In Disk Utility you can create an encrypted disk image - it's a .dmg file - that requires a password to mount. This obviously doesn't encrypt the whole home directory. But if you want to keep a set of files or folders encrypted, it can do the trick. You can even save the image's password in your account's encrypted Keychain, put the file in your login items so it automatically gets mounted whenever you log in. You don't even have to enter a password. Although you might not to do that if you want more security. Another question mentioned erasing files securely on the Mac. In addition to Secure Empty Trash, which according to Apple completely overwrites files with meaningless data - and I will vouch for that because it takes about 20 times longer to empty the trash when you use it - you can also securely clear all the free space in a hard drive. Disk Utility to the rescue again. Select the drive, go to the Erase tab - oh, that's right. I have seen this setting. Then you can erase free space with a seven-pass or 35-pass overwrite. Finally, if you boot to the OS X installation disk, you can run Disk Utility from the menu bar and securely erase the whole hard drive with seven- or 35-pass secure deletion. No DBAN needed. So Apple obviously gives you a number of ways to get this done.

Steve: Yup, and Brad pretty much covered the bases. Again, I wanted to acknowledge everybody who wrote in with various flavors and pieces of that. I mean, from what he said, and being a person who doesn't want to install software I don't need, I love the idea that you can create essentially an encrypted partition, one of these DMG files, and put things in there knowing that, if you remove the password from it, it's really going to be safe. Also remember that, if you delete files from there, you're not leaving them sitting there in the clear on your drive because Apple is encrypting them on the way to the drive, so they're always encrypted. So you essentially have sort of the equivalent of Secure Delete for free.

Leo: Right. Yeah, this is really a good technique. Also you can make a sparse encrypted

image so it's small, but can expand to accommodate whatever files you put in it. And when you mount it, it mounts like there's a drive there. So it just shows up as another drive. So it is actually a very good technique.

Steve: Nice.

Leo: Steve Hendry of Kitchener, Ontario says: "Steve missed an obvious solution (maybe)": Hi, folks. I've been an insatiable listener from the beginning - another #1 listener. You're all #1s. Steve's knowledge never ceases to amaze me. I hope the show never stops. One thing that surprised me, though, is his solution to the recurring question of how to provide both WEP and WPA access without risking compromise of the WPA side from the WEP access point. Steve's repeatedly described what seems to be kind of a kludgey solution involving three routers. Why doesn't he recommend using one of the free Linux firewall solutions - IPCop, Endian Firewall, Smoothwall - that allow separate networks to share an Internet connection without the untrusted network being able to see the trusted one. Both of these forks of the original Smoothwall install into an old PC with multiple NICs - you do need two NICs, I guess you might need three in this case - and allow up to three isolated networks with each less trusted network being unable to see the more trusted network. They are full-featured firewall routers in their own right, as well, and a great use for an old Pentium 2 or 3. I might also add you could use Astaro Security Gateway for this. That's Leo talking. Endian is available as a hardware appliance as well as a free distribution for PCs. Setting up one of these seems to be a lot more straightforward and elegant than rigging multiple routers together for the same purpose. Am I missing something? Keep up the good work. Love the show. Wouldn't be without SpinRite, either.

Steve: Well, he's absolutely right. I don't think this was an obvious solution, but I'm certainly aware of it. I guess the issue is for a high-end user, for somebody who has a PC, can install multiple NICs, wants to go into a Unix-based solution, absolutely this makes sense. Except that then you still need your wireless radios. So presumably you'd have a WPA router and a WEP router still. So really I don't think you've solved any problems because...

Leo: Well, and the router is doing essentially the same thing as the security gateway. So you've used up a computer, I mean, the router's a 40-buck way to do this, I guess is what I'm saying.

Steve: Yes, exactly. And so the reason I like what I'll call the "plastic consumer box" approach, just taking three routers and plugging them in in a Y connection is - that solves the problem. And this replaces the Internet-facing router, which splits the connection to a WPA and a WEP router. But you needed one anyway. So I didn't mean to snub all of these really nice turnkey solutions, and of course Astaro is, as you mentioned, Leo, is one as well. But you would still need two more routers, one for each of the WiFi formats. So you haven't really made anything simpler, it seems to me, although you've got a lot more configuration power, although a lot more configuration responsibility, as well.

Leo: It's very powerful. You can do a lot more with that. Yeah, I mean, and you still - and by the way, you still have the triangle. I mean, the content is basically the same, it's just using a different appliance to do it.

Steve: Yes.

Leo: Joe in Sacramento, California has some additional clarification about built-in Mac encryption and an enterprise security question: On the last listener feedback show, Leo was asked if he knew of anything that would encrypt a folder on the Mac. You can use Disk Utility to create a new disk image with a 25-bit AES password-encrypted encryption. You specify the image size, like 2GB. It creates a file of that size that's encrypted, which you can then open and write files to and close when you're done. Best of all, it's part of OS X. Well, and I should say the sparse image is probably more economical. It grows to accommodate what you need.

Steve: Yeah, I love that. I love that solution.

Leo: Yeah. That's what I use, encrypted sparse image DMGs. And it's very useful. I actually keep a bunch of notes in those things, with serial numbers and stuff. And that's - and I keep it completely - I feel secure.

Another note about enterprise security, in my work they've implemented full disk encryption using Check Point, I think. It slows things down. We've had some computers crash because of corrupted encryption information, like a FAT table. My question is, why not use Windows' built-in, enterprise-ready EFS? Do you know why? Have you tried it?

Steve: Well, it's interesting. This follows on some work I've recently done, which I will be sharing with all of our users before long. I found an incredibly nice, free, whole system encryption solution that does preboot encryption, where it alters the boot sector and points to some fixed file locations on the drive, and essentially does on-the-fly encryption/decryption for a system that doesn't have an encrypted hard drive. And it works beautifully with Windows. The reason I - and I explored using EFS. This was for a specific application I was configuring about a month ago. The problem with EFS is when you pull a file out, it stays encrypted. And normally what you want is you want the hard drive to be encrypted, but not exports from the hard drive. And so, specifically, I wanted a system to be safe. But if I took, if I copied a file, for example, to USB, I wanted it decrypted in the process and to be transparent. Whereas EFS actually uses file attributes, tags this as encrypted, and you get an encrypted copy that, you know, you can't use. I mean, which maybe what you want is to keep exported files from being decrypted on the fly. But that wasn't, in my case, the application I was looking for.

So this thing I found, rather than teasing our users I'll let everyone know, is called FREE CompuSec. I researched it extensively and will be doing a show on it before long. But if anyone wants to go poke around at it, that's the name of it. And I have checked out the security of this thing, and it is - they really got it nailed. It is nice. And I even went, I mean, I've even benchmarked it because I wanted to find out what would be the overhead associated with doing software, on-the-fly, encryption/decryption of the whole drive, which is what this thing does. Literally the entire physical hard drive, no matter how many partitions you divide it up into, no matter what you do, it starts at sector 0 and runs an encryption across the entire drive when you put it into that state. And I don't have the numbers in front of me because I've got them written down for the show. But it was like 9 percent overhead. I mean, nothing. It was not - you couldn't feel the difference at all. It took maybe 326 minutes to do - no, not 326 minutes. What I did was I benchmarked a highly frag- the defragmentation of a highly fragmented drive, both with and without this. And the increase was surprisingly minimal to add this on-the-fly encryption/decryption. So we'll be talking about that soon.

Leo: Wow, neat. Wow, very interesting. I can't wait. Our listener Glen in Denver, Colorado is in a hurry to login. Regarding Windows SteadyState, he says: My biggest interest, in addition to customizing what's retained and what is preserved, is how long the restoration

process takes. And we mentioned it does take a while. I always hate long login times required by machines that start up oh-so-many processes at login time. So this is the question of greatest concern. Is the logon process a matter of seconds, more on the order of minutes, how long?

Steve: Yeah, in my experience - and I didn't explore whether this was a function of the size of the cache. As I did mention in our SteadyState podcast, when you are going to install SteadyState, Windows asks you to defrag the drive, to bring as much unused space into one large, contiguous block. Then SteadyState, and I don't quite get why, but it just takes half of that. It's like, thank you very much. You had 50GB free, now you've got 25. And it's like, whoa.

Leo: That's annoying right there, I've got to tell you.

Steve: Well, you can easily, there's a nice UI, you can easily bring that down to 1GB or something substantially more reasonable. I don't know whether that speeds up the login process. The reason I didn't research it extensively is it wasn't that bad. I mean, the process definitely took longer, and it was more than seconds, but it was less than minutes. So maybe 45 seconds? Maybe, I mean, literally, about 45 seconds, I mean, enough so that - I'm the same way. I'm Mr. Login Speedfreak. And I was already saying that I don't run processes I don't need and so forth. So when this thing kind of like came to a grinding halt, and I'm looking at a blank screen with a cursor, it was like, okay, hello. But maybe it was 30 seconds. I mean, it was enough so that I knew it, but it wasn't enough so that I'm not going to use it in the application where SteadyState is really what I needed.

Leo: Yeah, okay. But, now, he's talking about boot time. Does that relate to boot time?

Steve: Well, yeah, because when you log on there's a, like...

Leo: It has to load in that partition?

Steve: No, I don't know what it's doing. It's definitely doing something. I thought maybe some other services were hung, so I went in and I...

Leo: So it is slow. I mean, it's slow.

Steve: It does slow down your login. There's no doubt about it. It slows down your login.

Leo: On the other of minutes?

Steve: No, like maybe 30 seconds.

Leo: Okay, that's not bad.

Steve: Yeah. Again, you know, Glen is really concerned about that. So I wanted to say yes, it

will. And I wanted to also mention that people can try this. I mean, it just - it does install nicely. And it goes away nicely, too. So it's not a big problem to give this a shot and see how you feel about it because it's easy to back yourself out of it.

Leo: Get back out, okay. Now, you were very patient, so you can hear Mark Livingstone's Quick Tip of the Week. This is the award-winner. Steve, he says, if people want to data-mine the Security Now! transcripts, Google can help. You ready? This is a really useful Google tip. I use this all the time. You type "site:" and then you can narrow its search down to a site. So in this case, if you type "site:grc.com" and then the word "transcript," which will narrow it down to transcripts, and then whatever keywords you want, boom.

Steve: And I've got to tell you it works because this is - I used it earlier today when I was putting the questions together for this AxCrypt.

Leo: Just to see if you'd ever mentioned the other one.

Steve: Yes. And nothing came up. And then I thought, uh, is this working? So it's like, wait a minute, maybe I'm fooling myself. So I put in, I don't know, VPN and went boom, and there was like, I mean, it's perfect, Leo. It's like every article - every article. Every one of our podcasts where I've mentioned VPN, thanks to Elaine transcribing them all, it's just bang. And thanks to Google, you can see the use of the VPN in context. I mean, it's like - and I have to say that I'm really pleased about this because I did mention last week or the week before that I was soon going to be adding full text search to GRC.

Leo: Now you don't have to.

Steve: Change of plans. I've decided that I just can't screw around with GRC when I've got CryptoLink that I'm so excited to get to. You and I talked about it six months ago, and I've made very little headway on it. So I decided, okay, we'll use this tip, site:grc.com space transcript space and then whatever keywords, you search Google, instantly people can find things in the podcast. And that way I don't have to go spend another six months implementing my own native search. Instead I can get to work on CryptoLink that I think a lot of our listeners will care more about anyway. So that's the plan.

Leo: That's excellent. Well, I have to say, once Google finds its way into your page, they do a great job. I use Google for searching my sites. Why do your own search? And I use WordPress and Drupal, and of course they have excellent searches. But Google does such a good job. I just use Google for it. Done is right. And many people, one of the things people complain about with podcasts, with netcasts, is they're audio or video, how do you find stuff? You're so smart to have the transcripts. I really should do that for all the shows because then it makes a netcast Google-searchable.

Steve: Right.

Leo: I think it's a really, really good thing.

Steve: Okay, now, read this #12 carefully and slowly, Leo, because this is extremely cool. It's the Amazing Idea of the Week Award. But our listeners are going to have to pay attention to

get this.

Leo: All right. Mike's corporation in Minneapolis wins the Amazing Idea of the Week Award: I just thought I'd write in to tell you about the enterprise security solution we use. I figured it was too esoteric to mention before. But since you brought up the use of VMware in Peter's response a couple episodes ago, I thought I'd share. In fact, our solution is just an inverted version of Peter's solution. What was Peter's solution?

Steve: Peter's was they had everybody running in VMware. Remember, he was the developer, and his company of developers were using VMware because they didn't want to have to constantly put Windows security patches in, which tended to break their build, their development build environment. And so the idea was they would keep the external Windows patched up and current, but then they would use a virtual machine image. And when they added somebody new to the project, they just give him an image, and he's instantly read to go.

Leo: Perfect. Perfect. Okay, well, he does the opposite, sort of, upside down. Here's what he suggests:

We run a virtual machine on each desktop. But instead of running the applications in the virtual machine and managing network security on the native machine, as Peter does, we do the reverse. We abdicate control of the real machine's network card to the virtual machine, so that the native Windows system doesn't use it and can't see it. We then establish a virtual network connection between the native Windows system and the virtual machine, so that all the Windows network traffic is routed through the virtual machine. Inside the virtual machine we run OpenBSD, which is a security-hardened version of BSD Unix. This effectively puts every Windows system on the network behind its own Unix firewall. This is actually brilliant.

Steve: It is so cool.

Leo: I have some questions for you about implementation. But I get the idea. This way, even if a rogue system were to be plugged directly into our network - oh, so this is the advantage of doing it individually on each machine - there's a firewall between it and every other peer on the same Ethernet segment. An OpenBSD firewall. The main advantage with this inverted approach is that graphic-intensive apps running on the native Windows system have no performance penalty. Except for, of course, the RAM that's used by the virtual machine. But otherwise they have full...

Steve: Ah, but that's where the beauty of OpenBSD comes in. He's about to talk about that.

Leo: Oh. We've also found some additional advantages using OpenBSD in the virtual machine instead of Windows. First of all, no additional Windows licenses are required. Because it's free, it's open source. And here, listen to this. The OpenBSD system can run in a virtual machine with a relatively small CPU and memory footprint, less than 32MB. You know, it's funny. I mean, that would be a lot a few years ago, but that's nothing on a 2GB or 3GB machine. The network packet filtering is much more configurable than what's provided in stock Windows. And I'll vouch for that. BSD has a great firewall. The network admins find that bulk configuration updates are much easier for Unix-based systems than for Windows-based systems. The system can be completely locked down by the admins without any fuss. Not even the most advanced Windows power users complain they're not

allowed to reconfigure the OpenBSD. Of course not. They don't want to get in there.

Steve: Yeah.

Leo: This is clever. Now, but I have some implementation questions.

Steve: So essentially, just to clarify, it's exactly like a personal firewall, but you're using OpenBSD running on a Windows machine as your personal firewall.

Leo: It's almost like you have a UTM for every desk, its own UTM, because - or however you're configuring that security. Now, here's my question. Okay. So I'm running Windows natively. I'm running all my apps natively. How do I tell my desktop Windows to go through the virtual machine for its network access?

Steve: I have no idea.

Leo: I mean, I like that idea, but that's what you need to do; right? You have to tell the Windows system, oh, no, your network isn't coming from your hardware Ethernet card, it's coming from the virtual machine.

Steve: Exactly. Somehow you've got to get the VM to publish a virtual network interface so that that's what the hosting Windows system can see. I have no idea how you do that. I mean, I don't know that you couldn't, I just never tried it before.

Leo: Yeah, because normally when you use a VM you're bridging your network access through Windows.

Steve: Correct.

Leo: The Windows which has hardware to the Ethernet, the NIC, has network access, and it bridges it over to the virtual machine.

Steve: Right. He did mention in the original email, and I think - it looks like I maybe have cut that off - where he said he would tell us how to do it if I want. That's right, he said he would tell anyone who wanted to know how to do it. And I thought, well, that's not going to work well in a question. But I think I need to write back to him and say, okay, give. How exactly do you do this?

Leo: Well, I think this would be a good topic for a show, is just let's talk about how to do this.

Steve: In detail, yeah. And what I love, again, is like, there are some personal firewalls that are 32MB. I mean, that take up a huge amount of RAM. And the beauty of Unix is that it is so small. I mean, it's running in people's routers.

Leo: And this is, I mean, you can - hardened Unix distributions are widely distributed. And I think OpenBSD is an extremely good choice, not only because it's hardened and it's secure, but also it's less likely to be known by many Windows-based hackers, or even Linux-based hackers. It's something a little different. But the other thing that worries me a little bit is you still have this hardware NIC and Windows, and they're sitting there right next to each other. You've really got to kind of find a way to keep Windows from looking at that NIC.

Steve: I would think, I mean, again, I don't know what they're doing. But you can certainly unbind network interface cards from Windows. I mean, there is - there's still this notion of binding of protocols and hardware.

Leo: So maybe you can bind it directly to the virtual machine.

Steve: Exactly. And you don't bind it to Windows. So Windows just doesn't see it at all. And then if the VM is able to publish a virtual adapter, then that's what you bind the Windows networking protocols to. Anyway, I think this was so cool, very clever. We're going to find out how to do it. And I agree, Leo. Well, the other thing, too, is that this could potentially, since it's now virtual machines are, I mean, not only are the virtual machine containers themselves free, especially if they've got OpenBSD in them, but we know, for example, that Windows Virtual Machine Server is free. So this is potentially a 100 percent free solution.

Leo: Yeah, or VMware. You could use a VMware player and VMware appliance.

Steve: Exactly.

Leo: Yeah. I wonder what - well, that's the other thing. I'd like to know what he's using.

Steve: We're going to find out. We're going to find out.

Leo: Is it VMware? Is it Windows, Microsoft's Virtual Machine? But do they still call it Virtual PC? What do they call it? I can't remember.

Steve: Virtual PC, last time I - yeah.

Leo: Well, I'm looking at VMware's virtual appliance marketplace, and they do have OpenBSDs. In fact, if you go there, you can look at their - they have a lot of free appliances, including a whole category of security appliances. So, I mean, there's a ton of choices there, including Astaro, OpenBSD with VMware tools, NetBSD, Stockade, I mean, there's a ton of commercial - and these are all free. Smoothwall...

Steve: It may well be that this evolved from someone using one of those and saying, hey, wait a minute, why can't we...

Leo: Yeah, go the other way.

Steve: ...unbind Windows from the physical container, I mean, from the physical interface and bind it to a virtual interface.

Leo: Yeah. I wonder if anybody else has thought of this? It's a very clever idea.

Steve: Yeah, I love it.

Leo: Yeah. Okay, yes, you do, you win, Mike. I don't know who Mike's corporation in Minneapolis is, but...

Steve: No, he didn't say.

Leo: He probably doesn't want anybody to know.

Steve: But I'm going to track him down.

Leo: Wow, really great. Hey, this is a long episode, but I think a really good one. We thank our new sponsors, Audible.com; and we welcome back our old sponsors, Astaro.com. Great to have you both on. And some great questioners. Thank you all for your questions. If you'd like to ask Steve questions, you can do it right on his site, GRC.com/...

Steve: Feedback.

Leo: Feedback. I never can remember that. Of course GRC is the place to go for SpinRite, Steve's bread and butter, his day job, that great hard drive maintenance and recovery utility that everybody ought to have. If you've got a hard drive, you ought to have SpinRite. You must know that by now. You can also go there to get the 16KB versions of the show, for people who don't want to download a giant show, or want to store it somewhere compactly. With 130 shows, it does add up. You can get that from GRC.com/securitynow. And also Elaine's transcripts. And don't forget that search tool [site:grc.com transcript {keywords}] because that's cool. You can just make that a search link that would automatically do that on your site.

Steve: Yeah, that would take five weeks.

Leo: Just pretend you wrote it.

Steve: Because it'd have to be perfect. No, no, no.

Leo: Just pretend you wrote it. And just, you know, oh, I think you could do that pretty

easily. But anyway, all right. We'll let people do - that's an assignment for home. Your homework assignment. Hey, Steve, thank you for a wonderful episode, and we'll talk to you next week on Security Now!.

Steve: Talk to you then, Leo, thanks.