Listener Feedback Q&A #17

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-084.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-084-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 84 for March 22, 2007: Your questions, Steve's answers.

Security Now! is brought to you by Astaro, makers of the Astaro Security Gateway, on the web at www.astaro.com. And by Nerds On Site. Looking to grow your IT service business? Find out how Nerds On Site can help. Visit Iwanttobeanerd.com.

It's time for Security Now!, and because it's Episode 84, that's good news. That means it's one of our divisible-by-four episodes. Every fourth episode we like to answer your questions. Steve has a passel of them. Hello, Steve Gibson.

Steve Gibson: Hey, Leo, great to be back with you.

Leo: It's nice to have you. You've been great, by the way; and I don't know if people know this, but Steve has been doing a regular segment on my radio show, as well. And it's just been great. It's going over very well. It's kind of a mini Security Now! because it's only six minutes. But still, I think it's getting the word out to a wider audience, and that's kind of important.

Steve: Yeah. It's really cool, too, because you've got a whole different, you know, a different geographical spread. You're on XM Channel 152, I think it is?

Leo: Yes. I'm really happy about that. All six hours of the show every weekend.

Steve: Did you happen to mention GRC and ShieldsUP maybe, like, early in the show on Saturday? Do you know if...

Leo: Could well be. I don't know. I don't remember. Why, did you get a little...

Steve: Something, yeah, something happened on the server. It's like, whoa, it's like in the old days of Tech TV. Whenever you'd mention GRC, like I'd just have to hold onto the edge of the desk.

Leo: Oh, I'm glad to hear that. If it was during show time, that's probably what it was. I don't know what else. Anyway, yeah, because, well, we're now all over the country in 13 or 14 markets. We just got Washington, D.C. I mean, it's really – it's growing very rapidly. So it's a big audience.

Steve: Fantastic.

Leo: Yeah, I'm really happy about it. And I'm happy to use it to expose people to some of the TWiT, you know, the best TWiT folks like you and Amber. And really, that's a neat opportunity, too. Dick DeBartolo does it. But let's get to our – oh, before we do, hey, some happy news. Last episode we said goodbye to Nerds On Site. They had only bought a three-week schedule. We think they're a great company, and we were really glad that they came on the show. And, you know, I think for a smaller company, I understand it's a big commitment. So we were happy to give them a three-week schedule. We don't normally do that. But they've had such success, results with their ads that they're back now for three more months. So...

Steve: Wow.

Leo: ...I'm thrilled. That's good news.

Steve: Very cool.

Leo: It just confirms what we know, of course, which is that people who listen to this podcast are very active and pay attention. And the people who sponsor it get the results because, you know, it's a good audience. So let me just mention, we're sponsored, once again, not only by Astaro, who is of course still with us and will be through the rest of the year, but by the good folks at Nerds On Site. Iwanttobeanerd.com. Maybe you could explain what they are because I'm not exactly sure, Steve. It sounds like it's kind of a guild of tech support, IT people.

Steve: Yeah, I think the word is "federation." They're like a federation of individual consultants who have this organization that sort of provides them with an umbrella identity. They get, you know, I don't know anything about the contractual details, but I do know...

Leo: But you get to keep your own business. You're still doing your own thing.

Steve: Exactly. But certainly there's some sort of fielding of leads. And they hold educational seminars. They have get-togethers where they all pull together. You know, I've done a deal with them that allows the Nerds to use SpinRite to help their own customers. So it was like a special expanded site license kind of deal.

Leo: Oh, isn't that nice. Oh, that's neat.

Steve: Yeah. I just think that they're, I mean, I know for a fact that there is a tremendous need for this kind of business. And certainly the quality of the people you get to have come out and help you matters a lot. Frankly, I've not heard great things about that Geek Squad group that seem to be doing that. People talk about long lead times and then not really great performance.

Leo: This is not them. Don't get confused.

Steve: Exactly.

Leo: This is Nerds On Site. One of the other things I love about it, it's very – most podcast advertisers are very nationalistic. They buy the ad mostly for the U.S. market. But Nerds On Site's in Canada, U.S., Mexico, England, Australia, South Africa, and Bolivia. So...

Steve: Wait, wait, and India. I just happened to notice that...

Leo: India, wow. And we're there, too. So that's one of the reasons podcasting is so good for them. Anyway, we thank them for their support. If you are a nerd, you're in business for yourself but you don't want to be in business by yourself, focus on your passion, not the burdens of running a business, with the help of Nerds On Site. No matter what you do, PC to Mac, Cisco to Oracle, fix-it, website design, programmers, product managers, project managers, sales, trainers, security experts, antivirus gurus and more, they especially like those nerds who troubleshoot, who tear apart and rebuild their own systems in their spare time. Iwanttobeanerd.com. Register for a nerds-only meeting in your area today. Iwanttobeanerd.com. We should make a little jingle for them. Iwanttobeanerd.com, yeah.

So let's get – because we have a bunch of great questions. I just love the questions that we get.

Steve: Yes. We have no errata this week. Well, actually there was some, but I sort of incorporated them into the Q&A because the errata were people making notes or comments and things. So we'll deal with that in the Q&A. I did want to share one fun SpinRite anecdote that put a smile on my face. This is from someone named Hareem, it looks like Haque, H□a□q□ -u-e. He says – the subject of his email was "Thanks for making SpinRite." He said, "My name is Hareem Haque, and I am a computer tech working with a firm here in Toronto." So he's up on the East Coast of Canada. He said, "I would like to say that ever since I bought your product life has been great." Yes, we fix people's lives, as well. He says, "The firm keeps an old Dell server as its primary data server, and the hard drive on the server was acting strange for the past few months. A few weeks ago the disk drive was on the verge of death. However, I ran

SpinRite on the server, and within 12 hours the drive was working like it was new. There were no signs of data loss, and that awful noise was no longer there." Then he says, "My boss was so impressed with the work he gave me a promotion. So I love you guys, man. The best $89 I ever spent. Keep up the good work."

Leo: Oh my gosh, that's really great, that's really great.

Steve: I just love that.

Leo: Very nice, happy stuff. SpinRite, of course, is Steve's product, and you can get that at GRC.com. I use it. Nerds On Site use it. If you have a hard drive, you ought to be using it, too.

Steve: Well, and it fixed your computer a few weeks back.

Leo: It did save me. I'm still using – by the way, that drive that it fixed, I'm still using it. It's recording reliably now. Haven't had a single problem ever since. So it worked. It worked.

Steve: Love it. Love it.

Leo: I didn't even retire it. I thought, well, it's fixed. I don't need to get a new one. Which is a good thing because it was a – oh, no, it wasn't a Raptor, it was the second hard drive that failed. The Raptors are the editing hard drives. Anyway, let's get to our questions. We've got quite a few of them here, starting with Security Now! listener Ian Chapman of Calgary, Alberta, Canada. He found newer versions of that stealthy Wireless Zero Config Update we were talking about, the one Microsoft didn't push out.

Steve: Which we keep talking about and trying not to talk about, but we can never get away from this topic.

Leo: The subject that will not die. KB923154, that's Knowledge Base article 923154, has slightly newer versions of the Wireless Zero Config files than KB917021, newer by four days, the 22nd of August as opposed to the 18th; and a later build, Build 2979 instead of 2977. The files seem to be the same size. They're both updates. The later update also includes updspapi.dll, an old DLL from 2005 but still newer than the version on my up-to-date patched system. I discovered these newer versions while perusing the RyanVM update packs to see if they included the 917021 files. In case you don't know, and I didn't know this, the RyanVM packs are used to slipstream all XP patches into a new Windows install disk, a very handy thing to have. Thought you might like to update the Security Now! Episode 81 notes yet again.

Steve: Yet again. Okay. Well, so what we have is we have an update to the update, neither of which you would normally get when you were keeping your Windows up to date using the normal Windows Update facility, even if you were accepting everything that Microsoft wanted to do to your machine. So what we advised people of last week was this 021 Knowledge Base article that has files four days older than the one that Ian found, this 923154. So I will put a link to this in today's show notes for this Episode No. 84.

It's worth mentioning, though, that this is what Microsoft calls a "hotfix," or a "hot patch," on the existing one. They specifically say that it's in case you have authentication problems with your Wi-Fi, it updates something called EAP, which we just touched on briefly back when we were doing all of our Wi-Fi coverage. That's the Extensible Authentication Protocol which WPA encryption allows. It basically allows different types of authentication to be easily added to the Wi-Fi protocol. Microsoft has a bunch of their own authentication that they like to use on their system. So there are situations which they discovered where this sort of reauthentication will fail if you don't have this hotfix. They specifically say don't bother with this unless you have this problem. But it seems to me like, well, it's probably a good thing to do because you get newer files. So I can see why RyanVM is using these. And I would say this is not nearly as critical to do, if for any reason it's not easy to do. But it's worth doing because then you're going to get more things fixed.

Leo: You know, and for all we know that newer file just has – they changed a name of a menu item or something. I mean, it may not make a big difference.

Steve: It could be a small thing that may not affect most people who are not using, like, one of these strange add-on authentication protocols. I just want to let people know that it's there, and I hope we never talk about this again.

Leo: We're done. Maybe. David Weiss of Redmond, Washington, raises the following point about full radio silence. In Episode 83 you mentioned how to maintain what you call "full radio silence" on a Windows machine. Now, I'm a Mac user. Couldn't believe it was so hard to turn off Wi-Fi on a Windows machine. It's true because on the Mac it's on the menu bar, you just pull it down, you say turn off Wi-Fi. After I blogged about it – and by the way, I should point out that many laptops have an on/off switch, which is an even easier way to do it. After I blogged about it, one of my astute readers pointed out that what you were talking about was radio silence when Wi-Fi is on, not trying to turn it off. Ah. I think the name "full radio silence" might be misleading. At least it was for me. Maybe you'd want to clarify this, at least for others that might have been confused like me.

Steve: So, yes, so I wanted to put this into this episode exactly for that reason, to say that – or to draw the distinction that when I said "full radio silence," I actually did mean it in the sense of the radio is on, but nothing is being sent out. Because that's been the challenge that we've been talking about for now it's five weeks, is trying to get Windows to allow your Wi-Fi to remain on, but to be quiet about it, even when you're connected or not connected. Because remember that, even when you're connected, it's still sending out packets, seeing if it can find a better connection, unless you say, no, just be happy with what you've got. Don't be talking about the networks that I've hooked up to in the past.

So like you, Leo, my laptops have an on/off switch. I would recommend for people to get in the habit of just turning the switch off. Or you can normally disable Wi-Fi, depending upon which Wi-Fi manager you may be using on a laptop. Some of them have add-ons in addition to Microsoft's. There are different ways you can actually turn off the radio. Being a fanatic about battery life, I like to do that all the time just because anything that's on is taking its little share of life from the battery, which as a cordless user you'd like to minimize that. So turning the radio off is certainly the best of all worlds.

Leo: That's true silence.

Steve: That's right, yeah, then it's been fully gagged as opposed to, you know, sending out all

these little beacons and probes and things.

Leo: What we were talking about is full radio silence while still using Wi-Fi.

Steve: Yes, or being able to, or at least having the Wi-Fi radio enabled. Whereas in the default case, Windows is just blabbing like crazy.

Leo: Right. Maybe just in the system tray you just right-click on the Windows Network little icon there and say disable the wireless, and then it'll be turned off.

Steve: Disable, right.

Leo: Although, as I said, it's really great when there's a switch on the side. That's the best way to do it. I think that's for airplanes. So when you get on the airplane, you just switch off your radio. Stefan Schmidt, listening to us from Mississauga, Ontario, wanted to share a spam solution and get our opinion. And I do have an opinion on this one. He says: After listening to you guys talk about spam during Q&A 13 at the end of 2006, the spam sent to our office email address has forced me to do something, to search for a product that could address this issue. He had tried the filtering features in Outlook and Norton to no avail. I agree. They don't work. What I found, he says, was a software program called Cloudmark Desktop at Cloudmark.com. It plugs into the Outlook. When I came into the office the next day and started up Outlook, to my amazement, and every day since, it gets rid of 99.9 percent of spam. Cloudmark's been around a long time. We've actually talked about it. I remember talking about it on The Screensavers years ago. He points out the software is based on a community of users who assist in identifying spam from which Cloudmark ranks the users and collects the data to filter out the spam. In other words, a community is working to find and delete spam. And since it's a community, the integrity of the spam filtering is tremendous. Have you heard of this product? What are your thoughts and concerns?

Steve: And I put this in here, Leo, because I was hoping, and assumed, that you would know about Cloudmark.

Leo: Oh, yeah. Cloudmark's excellent. Highly recommend. The way it works is you actually are sending your mail through their servers. You change the MX record. And they make it very easy to do. So that the mail goes through their servers. That's what I use. I use a very similar service called MailRoute. And the point is really that a professionally managed antispam service that is kept up to date, constantly worked on, is going to do a better job than anything on your desktop.

Steve: Well, for example, my own experience with Google Mail is that, because they've got the same sort of centralized view into the mail that's coming in, they're able to do a fantastic job of spam. Every so often, if your Google mailbox gets a piece of spam, you select it and say "Report as Spam." And that of course tells Google for everybody else's benefit that, you know, this is spam that exists with this particular profile.

Leo: I've had less, ironically – and I agree, it's the same concept – I've had less good results with Google. I get spam every day in my Google mailbox. But most people report

very good results with Google, so I'm not sure what's going on with mine.

Steve: It works well for me, although I don't have a widely public email address, either.

Leo: Yes, you see, you're not a target.

Steve: So the takeaway from this, I think, is that if we've got people who – oh, is Cloudmark free?

Leo: It is not.

Steve: Okay.

Leo: And actually there's one that works very similarly that is, in my opinion, just a little bit better. It's a little more up to date. It's called OnlyMyEmail.com. Same idea, collaborative filtering, taking off on Cloudmark. Cloudmark's very good. I think Cloudmark's been around for quite some time. OnlyMyEmail.com I think is 10 bucks a month, I'm not sure. And then, as I said, I use a commercial solution called MailRoute. But these all work the same way. And I think it's – I've always said the best way to get rid of spam is to not have it arrive in the first place. And the problem with a desktop antispam program is you're still downloading all that spam from your servers. These actually filter it out before it gets to your inbox on the ISP. So as a result you're downloading a lot less mail. In my case, a million messages a month less.

Steve: Well, and there is also the positive side effect that, as we know, some of this shotgun-sent email can be hazardous to your health.

Leo: Right.

Steve: It's not just hazardous to your mental health. That's been well established. But it can actually be hazardous to your system. So not letting it get near your computer is just sort of generally good for security.

Leo: Well, all these services will get a lot of the phishing scams. They will get a lot of the viruses. They'll actually strip viruses out. So, yes, you're absolutely right, these are security solutions as well as spam solutions.

Steve: Neat.

Leo: Yeah. Cloudmark is good. I highly recommend it. I haven't seen how much it costs lately. Kevin Rose was a huge Cloudmark fan. They're a good service. A listener using the Gmail handle of Diazamet, which is a risky handle – isn't that a drug?

Steve: Sounds like it.

Leo: In Warrington, U.K., is not impressed by Windows UAC. We talked about it last episode, the User Access Control. Despite your praise for UAC in Episode 83 of Security Now!, I still see the problem of security will be down to user behavior. And he's absolutely right. Of course it is. Users can screw up anything, can't they. As far as I'm aware, the UAC implementation by Microsoft does not require a password, unlike Linux or OS X. He's wrong there. The problem I see with this is partly the way in which Microsoft has implemented this – requiring the entry of a password is far more secure – and partly the mentality of a lot of Windows users. I do not mean to be condescending to Windows users. But for your average Joe, if the common response to these UAC dialogue boxes is to click OK, then it will become a reflex action – I do agree with him on that – because this is the action that will get rid of the UAC dialogue box the quickest. And therefore any security it offers will be quickly eroded. Both Mark Russinovich of Sysinternals and Jim Allchin of Microsoft state this is a design feature which is a tradeoff, as always. It's always a tradeoff between security and convenience. Unfortunately, nobody ever said security would be convenient. However, security is a necessity. And as long as Microsoft puts convenience before security, it will be flawed.

Allchin says, if security is not convenient, people would not use it. I say don't give people a choice. Whether or not they realize it, it's there for their own good. I know this sounds a little totalitarian, but a compromised Windows machine can affect all of us with spambots and so forth. That's a good point. It's not just the machine's owner. As Leo often stresses, change in user behavior is the biggest security feature you can have. But humans are creatures of habit, and sometimes it takes more than friendly advice to instigate change.

You know, it's interesting that you put this in because, you know, Kaspersky, who makes an antivirus software, in fact, one of the best antivirus softwares out there, recently said, quoted by ZDNet, saying that most users are just going to get so annoyed by UAC they'll disable it. And Kaspersky says that, without UAC, Vista is less secure. And Kaspersky's chief executive – now, remember, he's got a little axe to grind here, actually she, Natalia Kaspersky, said that her analysts have already found five ways in which malware could bypass UAC.

Steve: Well, you know, my comment to this, of course, and I put this in here just because I wanted to, I mean, it's a very valid point. He was a little mistaken saying that you didn't need to enter a password, unlike the Mac. In fact, on one of my Macs I don't have to enter a password. And in the case of Windows Vista, the idea is, if you didn't log on with the authorizing credentials, that is, if you're not logged on as an administrator – in which case, if you are logged on as administrator, you simply have to say Okay. If you're logged on as a so-called standard user, then you do need to provide administrative credentials. Of course, that just makes the burden of the UAC pop-ups more annoying rather than less. So, I mean, Microsoft is stuck because they are, as we've said before, and as I talked a lot about last week, they really are trying to make the system more secure. But they really are fighting the corner that they're painted into because anything they do that really changes the system's behavior to increase security will break things. So this is, you know, it's an evil, unhappy compromise, but it's arguably better than allowing changes to the system with no oversight at all. It's not perfect. They recognize, everyone recognizes that it's a tradeoff. It's going to be really interesting to see how it plays out. We really won't know probably for six months, and as we get more sort of feedback from people, was this useful or is it just, you know, annoying.

Leo: It does seem to bug you more than the Macintosh does. I've gotten used to it on the Macintosh. On both my Mac and my Windows machine I am frequently asked for an admin password. You don't get asked if you're running as admin on Mac.

Steve: On the Mac, isn't it only when you install something, yes.

Leo: Yeah, or you modify system files, yes.

Steve: Okay. And so on Windows it certainly is more pervasive than that. There are many other things that will cause that to pop up because of course Microsoft is reacting to, in every case, to specific malware that has abused something in Windows. And they're, like, saying, wait a minute, if that happens again, let's make sure this is the user doing it. So I do think that UAC is more – I don't know if I would say more granular, certainly more in the way in Windows due to Windows' own history of having so many exploited problems in the past.

Leo: Look, there's no perfect solution. Users are going to be able to get by anything that a company does. That's the problem. There's no way you can force a user to be secure.

Steve: Yeah, well, now I have to go and research what Kaspersky is saying because that's...

Leo: Kaspersky, that's a little scary, although they bring up that same old boondoggle about why doesn't Microsoft let us modify the kernel? They say the PatchGuard hinders their ability. I'll send you the link to this article in ZDNet.

Steve: Yeah, cool. I'll do some research.

Leo: And I thank Stephen Cerruti for sending it to me. Jonathan Lackman of Kansas City, Missouri has an oft-asked question: I've been reading your site for years. I presume he's talking about GRC.com. I'm an IT professional, and you've taught me a lot. I know he's talking now about GRC.com. I've also been listening to your podcasts since numero uno. However, when setting up my new iPod, only the last 14 show up in iTunes. Do you have any idea why they don't all show up? I can download them separately, but they aren't as nicely formatted and presented on the iPod.

Steve: And that's for you, Leo.

Leo: Shall I take that one?

Steve: Yes. It's here for you because – but it is, I hear this all the time, so I thought we ought to just tell people what's going on, and you're Mr. Pod Man.

Leo: And I make the decision, by the way, not to include all of them. With 84 episodes, it would be – the RSS file would be several hundred K. The way RSS works, it's really never been intended to have a complete listing. If you look at the RSS feed from any web page, it doesn't show every article that's ever been on that web page. It shows the most recent articles. And every person who creates an RSS feed has to make a decision, well, how many articles are you going to include?

Steve: I know the problem. The problem is we've deliberately designed a podcast that laid down some really significant, important, historical stuff, rather than just being sort of a news sort of thing. And so that's created a strong desire in the part of people who discover Security Now! to, like, go back and get them all.

Leo: I don't blame them. But the feed is not the place to find them. Now, I make a point of – my general policy is the most recent 20 episodes of every podcast. That's five months back. And it's really balancing the size of the RSS feed. Remember that every time some aggregator, including iTunes, requests the feed, it's downloaded from our site. And that can be quite a bit. That's several terabytes of downloads, and we're trying to manage that, as well. So what I do, if you go to TWiT.tv, in fact, just go to TWiT.tv/sn, for Security Now!, and every episode's there. It's on the web. It's not that it's not available to you. It's just that it doesn't show up in the RSS feed. And I think the reason people are confused is it's kind of Apple. I blame Apple a little bit because it's not clear that what you're looking at is an RSS feed. It looks like you're looking at a directory of all episodes. And that's not the case. It's not the case from our podcasts or anybody's podcasts. You can't do that.

Steve: So when he says – he says, "I could download them separately," so he obviously knows about that. But they aren't as nicely formatted and presented on the iPod?

Leo: That shouldn't be the case. It should be exactly the same. It may be something that iTunes does different with a podcast. It probably is, when it sees it as a podcast in the feed. Write to Apple. Don't complain to me. That's the way iTunes has decided – iTunes does some very strange things. It renames the files, it does some very strange things. But all of them are there. And frankly, you can listen to them all on the web page. It's the other thing we've done is we've made it possible to just click on an episode number. In fact, you can go by episode number. Just go to TWiT.tv/sn and the number. So if we say, oh, Episode 81, remember that, you can go to TWiT.tv/sn81. You'll go right there, and there's a player on that page. So I think that you can always, frankly, find it. It's not that you can't find it. I get this periodically. You know, with the Daily Giz Whiz we've done 270 episodes. There's no way I'm going to put 270 episodes in the feed. I mean, it's just...

Steve: I'm not going to be catching up with that number any time soon, am I.

Leo: Well, and nobody would probably want to listen to all 270, although we do hear from time to time people doing that. You're absolutely right. Security Now!, it's more natural you'd want to go back and listen. It's really the difference between what a feed is and what iTunes is presenting to you. And it really does look like iTunes is saying, hey, here's all the episodes. They're not. They're just saying what's in the current feed. Moving right along. I'm glad actually you put that in because I get that question a lot. For the first, you remember, for the first maybe year I put them all in there, and the file size was well over 100K. It was getting too big.

Steve: Well, and frankly, it would encourage people – I mean, okay. The way things are now, if people like the podcast, they've got to deliberately go back and yank these files off the server, which creates a nice tradeoff. If in fact the entire feed contained all the files, somebody just experimentally joining would suddenly find themselves downloading...

Leo: Oh, that's a good point, yeah.

Steve: ...84 monster files. It's like, aagh, stop, I don't want all this.

Leo: iTunes is smart enough to say you just want the most recent one, right? But you

could say no, I always want to get all the files. And that really would be a nightmare. If you look at any podcast, I don't know of anyone that actually puts all of their shows, if they have any number of shows, because you just can't.

Doug Smith of Albany, New York is busy catching up on back episodes after being hooked by the Honey Monkeys. Well, that was Episode 1.

Steve: It really was. I couldn't believe it was so long ago.

Leo: Way back. He asks: Here's my question. In your show about wireless security, when talking about brute force attacks, you mentioned a hacker could steal off with a sample of encrypted traffic and subject it to the attack. You made it clear that as long as you have a good password, you're probably safe from this kind of attack. But my curiosity is this. How does a hacker know when they've cracked the encryption? It would seem to me that they'd need to attempt to try to access your network with what they believe to be the key before they could really know. Doesn't that make the idea of them doing it from the comfort of their own secret lair somewhat impractical?

Steve: I loved the question because it's something I never addressed. It never occurred to me, because I know the answer, to make it explicit. And I also like it because we've much more recently seen exactly this happening with the cracks of protected content under Vista and HD-DVDs, where they were finding keys – and remember the idea was that the key would be somewhere in memory, and so they would scan through memory taking candidate keys and testing them against known encrypted content to see if it decrypted it. Exactly in an analogous fashion, we talked about – and this is specifically the WPA. Of course there were, you know, enumerable ways of cracking WEP, the first-generation bad encryption for Wi-Fi. The only known vulnerability for WPA is exactly what Doug cites here, and that's sort of the offline brute force attack, where you...

Leo: That's just because it's so hard to do that you need a lot of time to do it, is that why?

Steve: Well, it's because, yes, there is no obvious attack. So the attack that is available is that you capture some encrypted traffic, and then you do a brute force attack, for example...

Leo: You'd try every key.

Steve: Exactly, using dictionary attack, using alphabetic attack, using, you know, basically, I mean, maybe as much as going A, then AB, then ABC and so forth. So...

Leo: That's why, if you have a – that's why you keep pushing for a 64-character totally random key.

Steve: And as we know, if you go to GRC.com/passwords, you get exactly that over a secure link as raw material for using a key because it's just going to be garbage, and that's going to maximize the chance to the point where it's just not feasible of doing that kind of attack. Anyway, to answer this question and the exact analogous question in the case of hi-def decoding, it's always the case – at least in both of these cases. It wouldn't necessarily have to be the case. But in both of these cases when you get a decrypted blob, whether it's a chunk of

video that's been encoded in MPEG format, a frame of MPEG or a frame of radio data, a frame of Wi-Fi, suddenly the format becomes crystal clear. That is, all of these things, for example a Wi-Fi packet has a bunch of header information at the beginning before it's got whatever the content might be, whether it's ASCII or binary, and arguably that just looks like noise to a casual observer. But the headers have a rigorous set format that is very easy to recognize. So the automated software is looking at the beginning of the packet, in the case of Wi-Fi, or the beginning of a frame of MPEG data. And you know if it looks like complete nonsense, or if suddenly it all makes sense to software that knows sort of heuristically what the front of whatever it is you're trying to decrypt should actually look like.

Leo: It'll pop into focus. It'll be obvious. It'll just jump at you.

Steve: Popping into focus is a great analogy because literally, if you got the key wrong, it is completely random. As we know, encrypting and decrypting with the wrong key results in absolutely nothing coming back. It's just noise. So if suddenly you get structure at the beginning of whatever it is you're trying to decrypt, you know you got the right key.

Leo: Yes, absolutely. Dan Berkowitz, writing from somewhere in Pennsylvania, says: In my work I set up PCs for people. You should call Nerds On Site. A week after I installed – free plug. A week after I installed a Vista machine for someone, they told me they don't even pay attention to the UAC pop-up anymore. Okay, proof positive. And they hate Vista for it. All this brought me to thinking UAC might bring spyware infestations from 25 percent of PCs to 15 to 20 percent, you know, bring it down, but it's not going to be a whole lot more. The normal user that doesn't pay attention to the window is still going to get infected. Do you agree with this statement? It might be an interesting side note. And they will always find a way around it, probably in a week. Well, we have addressed it, haven't we, in the earlier question, but...

Steve: Yeah, exactly. And I just – I liked this because, as I said, we're going to have to see how the world reacts to this over time. This is an experiment that Microsoft is doing, clearly, saying to my mom and people who are not computer savvy, you know, popping this thing up and saying something is trying to mess around with your computer. Is this you? I mean, even that question, you could argue, is somewhat murky. It's very much like the problem that the personal software firewall vendors had when their software was popping up a dialogue saying something wants to talk to the Internet. It's this. Do you want to allow it or not? I mean, the great Achilles heel of that was people not knowing whether to say yes or no.

Leo: Yeah, and we saw that happen. That was very clear that people eventually either turned it off or gave up and just said okay, okay, okay, okay.

Steve: Or, as happened in the case of personal firewalls, once they had authorized all of their properly formatted programs, properly intended to be talking to the Internet software to do so...

Leo: It did calm down, yeah.

Steve: ...then it really did calm down.

Leo: But, see, that won't happen with UAC. It's going to annoy you every single time. It will never learn.

Steve: I'm afraid that might be the case.

Leo: Yeah. So it's not like it's going to ever calm down. What you see now you're going to see in five years because it's going to warn you every single time you install a program or every single time you modify the desktop file. You know, it doesn't bother me. In a way, now, I don't use Vista day in, day out, so maybe it would if I used it full-time. I don't. But I use it a lot. And it doesn't bother me. I just feel – in a way I just say, hmm, good, it's protecting me.

Steve: Well, yes. And, you know, from a power user standpoint, which certainly the two of us are, and many if not all of our listeners probably are, to a much greater degree than, you know, our moms, for me it's like I come to expect it. It's like, oh, okay, you know. I just did something, yes, yes, this is me. I mean, so for someone who understands what it's doing, it isn't that interruptive because like you, Leo, I recognize, ah, the system is there. I would want to know if it popped...

Leo: Of course, we're the ones who need the least protection.

Steve: Exactly.

Leo: We're the ones who could turn it off safely. Alex in Kentucky needs to accept incoming connections from SSH on port 22. SSH is the secure terminal.

Steve: Shell.

Leo: Yes, secure shell. He writes: I have an SSH server set up on my computer so I can create a secure tunnel for TightVNC. I currently have the server set up to use port 22. I use a 12-character password of random numbers and letters. I'm having trouble changing from the default port. Is there any significant security problem from using the default port? 21 I think is the default for SSH, isn't it?

Steve: No, that's Telnet.

Leo: Oh, that's Telnet, okay. So 22 is the normal port.

Steve: Correct.

Leo: Oh, he wants to use a non-default port.

Steve: Well, he'd like to change to a non-default port. But for whatever reason he says he's having trouble changing it from the default port. So he is on 22, the default port for SSH, and

he's wondering is this a problem. You know, he says, is there any significant security problem from using the default port. Well...

Leo: I'll tell you, when I look at my server logs, I see people try to log in on port 22 all the time.

Steve: Well, exactly. Now, but you don't have a server running on 22. Right?

Leo: I do. This is on my website. I use SSH to log into my website, of course, because it's secure. And we use the default port. The point is, if you have a good, secure password, these Chinese hackers are going to be working on it, but it's not like you can do a mass brute force attack. You get three tries, and then you have to start over again.

Steve: Right. So here's the issue, I think. He's advertising, his system is advertising that it's got SSH running, that is, an SSH server listening and accepting incoming connections, because he wants to be able to be outside of his own network and be able to connect in, give his credentials, which is secure over secure shell. It was well designed. So you end up with, you know, good, non-eavesdroppable security. But the problem is, he's saying, okay, when people don't know my password – and he knows enough to have a really bizarro 12-character password – am I in any danger? If his password is good, as you say, Leo, it's very burdensome for someone to crack it. On the other hand, it's still there. It's accepting connections. And so I would say he doesn't have a security problem. He just sort of has an annoyance problem. For example, he would be prone not to log what's going on on his router or his server because it's going to be, just exactly as you said in the case of your logging, it's going to fill up with people who go, oh, let's see if he's got a simple password that's in a dictionary. So he'll be prone to being attacked on 22. Not that he would be vulnerable because he did the smart thing. But people are going to be hooking up to him and trying. And that would annoy me if I was looking at my log and just seeing people hooking up to my port.

Leo: It's a little scary.

Steve: Yeah. It would just be...

Leo: It's a little scary; but that's, I mean, when you run a web server you have stuff like that. I mean, they're always trying to get in, you know. And they're trying to get into other services, too. I mean, they're always trying to do that.

Steve: But what I would suggest is, if he's behind a router, and he's mapped port 22 through, some routers allow you to map a different incoming port on the outside to a port on the inside. It may be that his SSH server running on his system doesn't like to change off of port 22. If he's got a router...

Leo: That's not the case. I don't know of any SSH server that won't let you easily do that. I'm not sure why...

Steve: Exactly. And I don't know what his problem is. But anyway, I guess, Alex, if you're listening to this, and I hope you are, not only for the benefit of all of our other listeners but for you, you know, make up your own mind. I wouldn't say you're under a great security risk. But

it would bug me if I had just random strangers all over the globe who I don't know hooking up to my port 22 and giving it a try.

Leo: When we were talking about Chinese hackers on the other episode, that's what they're doing. And I can tell. I look at the IP address, it's from China. I have strong passwords on there. I don't think a brute force attack – because you can't – it's not like you can run a program that will run through this...

Steve: At high speed.

Leo: ...at high speed.

Steve: Exactly.

Leo: It's a slow process. It has to be done by hand, essentially.

Steve: On the other hand, it's automated, and it's happening day and night unless you do something to prevent it.

Leo: Well, that's true. That's true. I guess if I saw a lot of activity I might change ports.

Steve: Well, and it would also be a matter of the value. You can imagine that, if this was a DoD IP or, you know, something really, you know, within .gov, that's probably much more prone to somebody methodically just saying, well, we don't care how long it takes. Maybe we'll get lucky one of these days. Whereas this guy, you know, he's just some random IP in Cox or wherever that, you know, doesn't clearly have that much value.

Leo: The other point is that, even if you move it to a non-standard port, these guys test all ports. So they'll test all ports for SSH response until they find your port. So if they're really determined to hack at you, they're going to hack at you.

Steve: Well, and in fact it may not be that anyone would even bother doing a brute force. There have been historically known security vulnerabilities in SSH. So it could be somebody looking for vulnerable servers, which Alex probably doesn't have. So it's just exactly as you say, Leo, someone scanning through IPs on port 22, hoping to take advantage of an insecure secure shell server. So they'll hook up, they'll try their little hack to see if they can bust through some buffer overrun in the server. And if not, they go away.

Leo: Right, right. You know, how hard you make your system, how hardened you make it, is up to you. And, right, it depends on the value of what you're protecting.

Mike Fattori, listening and writing in Toronto, writes: On a number of occasions in the past few months Steve has mentioned, somewhat parenthetically, that IP addresses cannot be spoofed because of the three-way handshaking involved with setting up a TCP connection. We recently had a Cisco firewall expert do some consulting for us. I asked him about IP spoofing, and he said it was all too real. He attempted to explain how it's done, but we

were interrupted before he completed his explanation. So is IP spoofing real, or are you and he talking about different types of spoofing?

Steve: Well, I'm sorry that this guy was interrupted because I'd love to hear from a Cisco firewall expert how IP spoofing is all too real.

Leo: He's probably talking about raw sockets.

Steve: Well, yes. He had to have been talking about something else. It's absolutely the case that, again, and we've talked about this extensively in the past, you know, on those podcasts that are not available on the – for easy download...

Leo: By the way, if you subscribe in iTunes from now on, it doesn't delete old forms of the podcast. So everything from now on will be in your iTunes directory.

Steve: And that's exactly how it was intended to operate. So anyway, the idea is, packets are just little blobs of data moving across the Internet. The only thing that most software looks at is the so-called "destination IP." The source IP is also there, always there. Every IP, that is, every Internet protocol packet, has that right up at the very front, the destination IP and the source IP. The destination IP is where that packet is going. In theory, the source IP is the IP of the source of that packet, which is where it came from. But nothing validates that as packets move across the Internet. So anybody who wants to emit a packet can pretty much make up any source IP that they want to, drop it on the 'Net, and off it goes. So, yes, that's spoofed.

Leo: But you can't have a conversation if you do that.

Steve: Yes, and that's exactly my point is why, when I specifically talk about the three-way handshake that sets up a TCP connection, the beauty of the security of that is that each end requires a roundtrip. The reason it takes three packets is that the initiator sends a SYN packet, a synchronized packet. The receiver sends a SYN/ACK, which acknowledges the receipt of the SYN, and contains its own synchronization to which the first party sends a final ACK back to acknowledge the SYN, the synchronization from the second party. So those three packets give each end a roundtrip. The only way each end can get a roundtrip is if all packets have the correct source IP and destination IP. So that TCP handshake prevents spoofing. Now, things that don't prevent it are, for example, pings, which can just be sent out to any random IP you want.

Leo: Or if you're a hacker who doesn't care about the return response, as in a SYN flood, you can spoof the originating IP because you're not having a conversation, you're just flooding.

Steve: Exactly. Exactly.

Leo: All right. I'm going to give you a hypothetical. How about in the man-in-the-middle attack? Couldn't a man in the middle modify the return IP address? He knows what the real return is.

Steve: Yes, absolutely. And in fact, that's what a man-in-the-middle attack would do is he would grab the packet on its way to the other party and change the source IP to his own. So that then the packet goes off to the other party, the other party responds back to him thinking that it's the first party. He then changes the source of that packet as he forwards it back to the first party to his own, basically knitting himself into the middle of a conversation. And by the way, that's exactly what proxies do. Proxies are man in the middle of TCP connections.

Leo: Oh, yeah, I guess they are. So in that sense certainly it is possible to spoof IP addresses. It's just not possible to spoof an IP address in a real conversation, that's all.

Steve: Right. And we're normally talking about something where you've got an encrypted PC connection which, if things are done properly, even prevents a man in the middle, i.e., a proxying of that connection.

Leo: Right, right. David Barnes from Basildon asks, what can we as users do about the continuing spread of excessive Java and other client-side scripting use? I'm just going to have to correct him here. There's Java, and there's JavaScript. It's not your fault. It's the people at Netscape who decided, oh, we'll call our language JavaScript and confuse everybody.

Steve: And you know, Leo, it doesn't even – it's got no connection to Java. It's not even – doesn't look the same. It's a made-up language, completely separate.

Leo: Well, I can't remember the original name, but it wasn't JavaScript. It was purely a marketing thing. Well, hey, Java's hot right now. Anyway, so he says "Java." I'm going to read it as JavaScript. I recently complained to eBay that the pages were not displaying correctly with scripting off. Well, as you might imagine, I was told I had to use scripting on eBay, a sort of "tough, we don't care, lump it" attitude. I then had a quick look at the JavaScript...

Steve: Script.

Leo: ...and the include files for a normal search results page. It totaled up over 300K. No wonder the page is bloody slow to load with scripting enabled. What else can us lowly sys admins and our users do? I feel like I'm being held hostage and dictated to in how I use the Internet.

Steve: This is where I put the needle down on my broken record, you know, and I just say, mark my words, this is going to be a problem. Not just the size of scripting, but it's going to be a constant problem. And I wanted to answer David's question because of course I'm sympathetic to it. As you know, I surf with scripting disabled, much as he obviously does. In my case, I've seen the same thing with eBay. So I've, using IE's sort of dynamic scripting enablement system, which is using these zones of trust that IE has, eBay is in my trusted zone, so scripting is enabled automatically when I go to eBay, but not by default when I surf to random sites that I don't trust. So basically he's talking about sort of the tyranny of web scripting. And I could not be more sympathetic to him. I mean, I absolutely agree. I think it's sad that we have these problems. Of course, now, Leo, I understand you take, as you've said recently when we talked about this, sort of, you know, your site requires scripting like eBay does.

Leo: Almost all sites do. It's just you can't do AJAX, you can't do a lot of user interface stuff. You can't validate forms. I mean, it just goes on and on and on.

Steve: And sort of all of that Web 2.0 stuff that you and Amber are talking about...

Leo: It's all JavaScript, yeah. Now, you can, if you really work hard, do a lot of it, as you've proven with your CSS, without any JavaScript, but it's a lot of work. And there is stuff you just absolutely have to use JavaScript. Now, what I would say is, yeah, there are JavaScript exploits. But they are few and far between. I don't think JavaScript is as dangerous as you seem to.

Steve: It's just, I'm not complaining about the danger, I'm just saying philosophically it's bad to load code from random websites you don't know.

Leo: But that's what the web is.

Steve: That's, well, it's what it's become. It isn't, I mean, it wasn't there originally.

Leo: No, if you just want static text pages, the web is fine.

Steve: Except that my site runs perfectly with no scripting. My ecommerce system, ShieldsUP...

Leo: But your site looks like it came from 1989.

Steve: Well, it did.

Leo: This is the tradeoff. More and more we want web-based applications. You're going to have to load code.

Steve: Okay. You're right.

Leo: So in my opinion what you should do, I mean, look at Java – as opposed to JavaScript – which is sandboxed. There have been some exploits, but nothing of any severity. You could make JavaScript much more secure.

Steve: Now, is Gmail JavaScript or Java?

Leo: JavaScript.

Steve: Okay.

Leo: Pretty much, well, you know, because you turn off scripting, almost every site uses scripting. Even if just for a rollover. Now, some of that's laziness. I suppose you could do it other ways. But it's pretty much accepted. And as we get to a richer and richer web experience, it's going to be more and more, not less and less. With Flash, I mean, Flash is scripting.

Steve: So David and I are losing the battle on this.

Leo: You're going to lose this battle. So I think the real trick is to really insist that companies that make these languages sandbox them, make them bulletproof.

Steve: Well, and it's one of the things that we briefly touched on last week with UAC. Microsoft has this notion, this concept, which is still in its infancy. But the idea is that IE or other browsers, and email clients, things that are chatty on the 'Net, things that are fundamentally less trustworthy, they will be running with less interconnection privileges in Vista, which doesn't give them the access to the desktop and to other Windows resources that more trustworthy applications have.

Leo: I think that's where we're going, absolutely. And I think that's a perfectly sensible way to deal with it.

Steve: And we've talked, in fact, about running sandboxes and sandboxing IE, or virtual machines, using virtual machines to create an environment of containment around these dangerous things.

Leo: Java's been around a long time. And you receive very few complaints about its security.

Steve: JavaScript you meant.

Leo: No, I'm talking about Java. Java is sandboxed.

Steve: Oh, yes, yes, yes.

Leo: JavaScript obviously has issues. The biggest issue is this most recent one where you could, if somebody hasn't changed their default password on their router, you can go into the router. And I think that that's a hole that can be fixed. I mean, I think it just should be fixed.

Steve: But it's a perfect example of what I'm saying, too. I mean, yes, I know it can be fixed. But it's a perfect example. You know, I'm running – my system is running scripts that I didn't really want it to run.

Leo: I know. No, I know. But that's the web. I mean, the question is, do you want the web

to be static text...

Steve: Yes.

Leo: ...or do you want it to be web services? Do you want applications to run? And I think people want applications to run.

Steve: Yeah, you're right.

Leo: A listener named John from Downers Grove, Illinois wonders: I followed all the Wi-Fi lockdown instructions from your recent Episode 81 notes. But now I see two new networks, "freetoguest" and "NRT-AIRPORT," both unsecured computer-to-computer networks. But they're not real. Network Stumbler doesn't see them. Any explanation from the guru department?

Steve: I guess that's us.

Leo: I don't know.

Steve: Yes. And I never made this explicit. But that Preferred Networks list that you can see in the dialogue box in the samples, there are two different lists that you encounter when you're using most Wi-Fi interconnection helpers, and certainly Microsoft's default one. There's that list of all networks that your computer can currently see. And then there's that different list called Preferred Networks, and those are networks it has seen in the past. So those you can – and that's what he's talking about here. He's got everything locked down, but he's seeing "freetoguest" and "NRT-AIRPORT" in his Preferred Networks list. All you have to do is highlight them and delete them. Highlight the next one and delete it. And they will go away. And now that you've got this thing locked down, they won't come back.

Leo: So this may happen from time to time that new networks enter that list.

Steve: It could because networks that you do connect to will be added to that list because Windows thinks it's doing the right thing by trying to reconnect to things you have explicitly connected to in the past. The good news is you at least now, with all these updates in place, even the one today, that we talked about today, you at least won't be broadcasting that you ever talked to those networks in the past.

Leo: And now our last question. Ryan Skelton in Portland, Oregon has a different problem with Windows UAC: I'm a serious computer user with multiple disabilities, and I must use assistive technology to enter text into all computer applications. My concern is that the UAC secure desktop may prevent my assistive technology application from entering text into the authentication fields. This is because it does that weird screen thing. I understand this is a tradeoff between usability and security. In my case, and I suspect many other disabled users out there, this usability is not merely a convenience but a necessity. Is there a way for an administrative user to specify that a particular program should be allowed to run in a protected desktop environment? If not, maybe I won't be able to use Vista.

Steve: Well, we never talked about – and this is a great question because we never talked about disabling all of this UAC nonsense. I certainly don't want to be promoting it. But this seemed a very valid place where a serious computer user is saying, I just, for whatever reason, I can't have these pop-ups. Now, backing off from that for a moment, I would imagine that any updates to his assistive technology would be updated to deal with this, and that there are doubtless ways of handling it. I'm assuming that. On the other hand, you could imagine that, if there were ways of handling it, that would be backdoors that would allow hacker technology to do the same thing. So what I do know is that many power users are familiar with utilities like Tweak UI. Tweak UI basically allows you to change even more settings than you can from the normal desktop. Well, there's a whole 'nother huge array of settings that are known as "Windows policies." There's group policy editor. Those are things – it's phenomenal how many other tweaks there are. And it turns out that being sensitive to what changes Microsoft was introducing with Windows Vista, there are a whole bunch of new policy settings that allow you to completely remove UAC intrusions.

Leo: And I believe you don't have to go that far. You can just turn off secure desktop but still have UAC.

Steve: Correct.

Leo: And that's probably going to solve his problem. I mean, he could certainly turn off UAC. But you can keep UAC without getting rid of, I mean, you can get rid of that blacked-out desktop without getting rid of UAC.

Steve: Yes. And if you did that, then you're right, then the assistive technology would no longer be cut off from the secure desktop environment that is deliberately putting a moat around itself in order to prevent it from being disabled. But I wanted, first of all, to tell Ryan that that exists in Vista so he could definitely use it if he needed to. And I wanted to point out for all of our listeners that there is highly granular control in the Windows policies world.

Leo: It's really cool, yeah.

Steve: Yeah, I mean, there's just a ton of stuff you can do. And again, sensitive to what Micro- because Microsoft never wants to break anything. So sensitive to that, they said we're going to have an intrusive technology, but we're going to give you all kinds of control. In fact, there's even, right up in the standard log-on profiles, not even down in the policy editing stuff, you're able as an administrator to just turn off the pop-up completely, turn off that acknowledgement with a single checkbox up in the regular user configuration dialogue. But there's much more you can do, as well. So I wanted to make sure that our listeners knew that that was all buried down there in Vista for people who did want, for example, and Ryan may have to, make that sort of change if UAC is really causing a problem. It isn't a reason for abandoning Vista.

Leo: I should point out, unfortunately, that all of these policies are available in a very easy-to-use, the local security policy, very easy to use in Vista Ultimate and Vista Business. But if you're a home user, you have to go into the registry and modify a registry key. So they don't want home users to have that kind of capability, I guess.

Steve: Probably just as well.

Leo: Yeah. I have a good article here from HowtoGeek.com that describes this in detail. So maybe I'll put that link up in the show notes there.

Steve: Oh, cool.

Leo: Yeah. It just talks exactly about how to do it and even has the key for registry editing. Well, that wraps up a list of 12 great questions. Before we wrap up, though, I do want to thank our friends at Astaro who have been sponsoring this podcast for a long time and now are up for the entire year of 2007. Again, we really – that support makes such a difference to Steve and me, I mean, really means that the show is working for them. And they work for you, let me tell you. Version 7 of the Astaro Security Gateway is out and amazing. I've talked about some of the features, the fact that now email encryption is centralized so your users don't even have to know they're doing it, it's just automatic. You've got SSL, VPN, makes it very easy to use VPN. It clusters now, so it scales up to 10 Astaro units in one without installing and load balancing. It's just really remarkable.

But the thing for the home user that I think is great is they've now waived the license fee for the v7 package so when you download the free Astaro Security Gateway as a non-commercial user, you get all of the subscriptions, including Astaro Up2Date, the antispam, the antivirus. They used to charge 79 euros for it. It's now free. I'll tell you, if you are in business and you want the best appliance to protect yourself, you've got to check with Astaro, www.astaro.com, or call 877-4AS-TARO, and you can schedule a free trial of an Astaro Security Gateway in your business. I use them, and it's just fantastic.

Wow, 12 questions, 12 answers, and some really fascinating stuff, too, I think.

Steve: Yeah, I love our Q&A sessions.

Leo: I really do, too.

Steve: Because they bring a diversity, lots of different things going on. You know, it closes the loop with our listeners. It's just terrific.

Leo: Well, Steve, we'll wrap...