SECURITY NOW!

Transcript of Episode #60

Listener Feedback Q&A #11

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-060.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-060-lq.mp3

Leo Laporte: Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 60 for October 5, 2006: Your questions, Steve's answers, #11.

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

All right, Steve Gibson, we are back. And we have an apology for last week. I'm so, so sorry.

Steve Gibson: Well, yeah. We're just both of us so distracted and busy. And of course, you know, we're recording this episode on Saturday early because you're off to Toronto again next week. And so for us it was yesterday that we were together at the Podcast and Portable Media Expo.

Leo: Wasn't that fun?

Steve: It was really great. I mean, so many Security Now! listeners and, you know, just general TWiT supporters were there. I mean, you know, my hand, well, it isn't quite, you know, fallen off from...

Leo: It's a little numb.

Steve: ...from shaking so many people's hands. But it was really neat to have that contact, yeah.

Leo: But I – and really it's my fault entirely, not Steve's. We had the podcast done. I just was a little fuzzy with all of the attention, and I just – I forgot. And I'll be honest with you, it was very simple, I just forgot. But I got it up when I got to the airport. I ran out of there because I had a flight. And I had a couple minutes to the airport and had found some Wi-Fi. Because we remembered – I think we remembered in the car. So...

Steve: It's like, oh...

Leo: ...as we're driving away.

Steve: I mean, I literally thought it was Thursday. I didn't even know what day it was.

Leo: I was confused, yeah. So, but it's not your responsibility. It's my responsibility. We had done it, so...

Steve: Yeah.

Leo: I, you know, as soon as I got to somewhere, anywhere that I could get it up, I did. In fact, they were boarding the plane, and I'm typing very frantically.

Steve: Well, and a lot of listeners were writing and saying, hey, what happened, where are you guys? Are you guys okay? And so anyway, so I want to thank everyone for your concern, and...

Leo: We're okay.

Steve: ...we really do try never to be late because I know it's important, and people have it sort of factored into their schedules.

Leo: Right.

Steve: Which is, you know, also very flattering to us, so...

Leo: Well, unfortunately it's the nature of a podcast sometimes. I mean, I don't want to say we're amateurs, but we're certainly – it's more of a hobby than a profession. And so sometimes things happen. And I do apologize. In a way it's gratifying because we know now that people actually listen.

Steve: Yes, and we both do take it very seriously.

Leo: Oh, yes.

Steve: So, you know...

Leo: Absolutely.

Steve: That's why we're recording this one on a Saturday morning, so that there will be something next Thursday.

Leo: That's right, because I'm off to Canada now to do a Security Now! [sic] right after this one. We do have – it's Episode 60. That's divisible by four, so you know what that means.

Steve: Yup, listener Q&A.

Leo: I think we've got a dozen good questions from our listeners all around the world. Starting off with Aabybro – I hope I'm saying that, Aabybro, Denmark – you know, I met some Danish podcasters while I was at Podcast Expo.

Steve: Oh, cool.

Leo: And we have some real fans in Denmark. Morten Rensen says: Where do I find the show notes for Security Now!? Simple...

Steve: This is sort of a simple, short question, sort of a little bit of a softball question. But it does come up. So I just wanted to let people know that on the Security Now! page every episode has its own box with a description. The first icon is the high-quality, 64KB audio. The second icon is the quarter-bandwidth, 16K, for, as you've put it, Leo, for the bandwidth-impaired. The third icon is always the show notes. And, you know, many shows don't have them. But from time to time we'll have one like we did last time, or actually time before, where we were talking about the VML exploit. And there, I mean, that page has been heavily read. Something like 8,500 readings per day, I think it was getting. So, yeah, so it's the third icon in for every single show is always the show notes. And then the following three are various forms of the transcripts that Elaine does. And in fact we met her for the first time. She came...

Leo: That was fun.

Steve: Yeah, she came out to the Podcast Expo, and so we were able to hang out with her, also.

Leo: Yeah. She's our transcriptionist, a wonderful person who does a very good job. And I have to apologize. On many of the other shows we have more complete show notes. I point to Steve's page for the show notes. But from time to time I will put, if there's something really important, I'll put links in the show notes on TWiT.tv, as well. And maybe I'll start doing more of that because, you know, it's really just a time issue. So we'll figure out some way to get more information there. So that – because I know a lot of people just go to TWiT.tv. In fact, actually, the truth is, a lot of people don't even go to any web page. They listen to it. It's automatically downloaded.

Steve: Right.

Leo: And we, on some of the shows, actually do put more complete show notes in the little descriptive field that you can see. If you have an iPod or some MP3 players you can see a descriptive field with extra text. And that's not linkable, if you're listening on a portable player. But at least you could see more, and I should put more in there. So I'll try. I'll do my best.

Steve: Well, and talking about time, Leo, you've just added another podcast; right?

Leo: Yeah, two more. Yeah, we have a new one from Paul Thurrott I'm really excited about, Windows Weekly.

Steve: Yup.

Leo: And I was talking with you about that yesterday. I really think that's going to be one of the top shows that we do because there's so many people interested in Vista. And Paul is so great. You were with me...

Steve: And he's not a Microsoft apologist, either.

Leo: You were with me, weren't you, when we met the Microsoft guy?

Steve: I was, I was.

Leo: There was a marketing guy from Microsoft who was part of the Vista program, I think...

Steve: And actually I'm glad to have met him. I've got his card. And he said, Steve, when – if you get pissed off at Vista, call me first.

Leo: He said it more gently than that, but that was the gist of it. We'd like to, you know, we're doing our best, we're trying our hardest, and we would love to have a chance to talk to you if you have any questions. And that's completely reasonable. It's nice to have a channel in there. And then I said, hey, great news, we're going to do a Windows Vista podcast, a Vista podcast, and Paul Thurrott will be doing it. Pause. Pause. And he says, oh, that's good. And to me, that was the reaction I wanted. If the Microsoft marketing guy had said, oh, that's great, I might not have been quite so happy. But Paul tells it like it is. And that's ultimately what the Microsoft fellow said. He said, well, one thing about Paul, he's honest. And I said, yes, that's why we have him.

Steve: Yup.

Leo: Windows Weekly. So we'll probably be covering...

Steve: And then you're also – I'm sorry.

Leo: We'll probably – go ahead.

Steve: And then you're also doing a new legal podcast.

Leo: We are. And you met Denise, as well, Denise Howell, who is a very well-known legal blogger and will bring some great legal minds in to talk about some of the big issues in tech law. Now, not just – not law in general, but there's sure a lot of tech law. And, you know, we've sat there on TWiT sometimes trying to wrap our minds around some of these legal issues and not done such a great job. Also Denise was kind enough to say, well, you do pretty well. But I thought it would be better to have somebody who actually has some training in this talking about these things. So that's coming out probably after I get back from Canada. I don't know if I'll be able to get it out this weekend, but I'll try. I'll try. I'll do my best.

Meanwhile, another question. And we got off on a sidetrack here. Brian Voeller of Ashland, Oregon writes: Considering the recent VML hole – that's what we were talking about in Episode 58, a very, very serious Windows hole which has since been patched.

Steve: Yup.

Leo: We're glad to say. Is it possible for a bad website to reregister that DLL through ActiveX and exploit it? Because that was our fix for it was unregister the VML DLL. I ask this because, if it couldn't be done without already having infected the system, why did Microsoft wait even one minute and use the automatic patch system to do what you instructed us to do? Couldn't they have just done that automatically? Then they could take their time and really go over that DLL with a fine-tooth comb. If that's the case, and considering how easy it was to disable the previous WMF issue, it seems to be to be criminally negligent on their part.

Steve: I like this question because it starts off suggesting that, well, if a bad website could use ActiveX to reregister the DLL. Okay.

Leo: Which it could, of course...

Steve: Well, okay. Let's stop right there. We know that ActiveX is itself inherently a huge problem.

Leo: Right.

Steve: I mean, ActiveX is downloading essentially a DLL code into your machine and running it. So if a bad website can use ActiveX to reregister a flawed DLL, well, it could just as easily do anything else it wants. So, I mean, I wanted to sort of, like, refocus on...

Leo: That's the least thing they would do.

Steve: Exactly.

Leo: I see what you’re saying.

Steve: I mean, yeah. I mean, doing that would be a very roundabout means of doing what they would really want to do, if any bad website could run ActiveX. What that means is, it’s running code it just provided your browser natively in your system. Well, you’re already hosed. I mean, it’s game over at that point. So, you know, shutting down ActiveX or limiting scripting so that you’re only allowing scripting for sites you trust, or switching to a browser that explicitly does not support ActiveX, you know, Firefox without an ActiveX add-on, for example, will make you substantially more secure, so you don’t have to worry about browsers doing that.

Now, the newer versions of Internet Explorer, of course, post-Service Pack 2, they will warn you when a site is attempting to provide your system with an ActiveX control and run it, and give you the opportunity, finally, of saying no, I don’t like this site enough, I don’t trust this site enough to allow that to happen.

Leo: All right, yeah. There have been in the past bugs that would prevent the certificate from showing up. And that’s really scary because then that’s similar to the VML hole. It means any program could do any – any website could do anything it wanted.

Steve: Right.

Leo: But that’s working right now, the certificate system; yes?

Steve: Yes.

Leo: We hope. As far as we know.

Steve: Well, but again, you’re still trusting your user ultimately to say, I’m not going to let this site run...

Leo: Well, no, that’s the point is that in the past they’ve been able to get around that warning.

Steve: Right.

Leo: So as long as you’re getting the warning, yeah, one hopes that you’re going to have people smart enough to say no. That’s another matter entirely.

Steve: Right.

Leo: Colin McWilliams, wandering around the U.S. somewhere, says: In Security Now! 52, Leo talked about downloading Hamachi Server. Then you talked about setting up your own private Hamachi network. I looked online to try to find the Hamachi Server but couldn't find anything like that. Hamachi is great, but I'm looking for a solution that does the same as Hamachi and allows me to control the network. Rightly so, since Hamachi's now been sold, you might have some concerns about it. But, you know, he wants to host the Hamachi Server. But where is it? I can't find it.

Steve: Well, we did address this once, but I wanted to come back to it because many people at the Podcast Expo yesterday were, you know, telling us what fans they are of Hamachi. They loved the fact that Security Now! turned them on to this great solution. There was some concern about Hamachi's sale, that, you know, Alex sold it to LogMeIn folks. And so I wanted to remind people that, you know, for what it's worth, I did talk to Alex Pankratov, Hamachi's inventor, father, designer, and ultimately seller, and he really did check these guys out and believed that they were really going to follow his philosophy of keeping this thing secure, not playing any games with people and, you know, doing the right thing. So for what that's worth, you know, he didn't just sell it to the first people who came along. He really felt like he vetted them completely.

As to the Hamachi Server, it turns out that that was something he was talking about on his website originally and had intentions to do some sort of a hardware-bundled solution. It would not have been ever downloadable software because he just knew he would never be able to control it from a piracy standpoint.

Leo: Ah, okay.

Steve: So he was going to do some sort of a box, the way Google has, like, their own Google Search appliance that you're able to purchase. He was going to do a Hamachi networking appliance of some sort, tying the software to the hardware. It never got past early alpha stage. The guys he sold Hamachi to, the LogMeIn folks, do now have that as something they could pursue. But there's been no indication of whether they're intending to do that or not. So it's sort of not something that anyone should plan on and/or expect to have happen.

Leo: So we probably shouldn't have said anything about it, frankly.

Steve: Well, yeah. We didn't know at that point. So I did talk to Alex again to find out what's the story on Server, and that's how I got the full update.

Leo: Scott of Cincinnati, Ohio wonders about virtual machine USB support: I plug a thumb drive into my computer and intend for the USB drive to be recognized by the virtual machine. How does the host operating system know the thumb drive is for the virtual machine and not for itself?

Steve: Well, this is a perfect question that follows from the issues we were talking about, about USB support within virtual machines. If a computer that is the hosting machine – obviously it's got hard drives. And you might have already plugged a USB thumb drive in, so it's appearing in the host machine. Well, any of the virtual machines could be asked to see that thumb drive as a hard drive. But what the USB support does, it's sort of similar to CD-ROM support where, when you insert the CD, who's going to own the existence of that CD once it becomes acknowledged by the system? So what USB support does within a virtual machine is it makes that support dynamic, so that when a USB device appears – and any USB device, not just drive devices.

Drive devices are sort of easier, and always have been, because a drive can be recognized by the host system, which you could then inform the virtual machine to be able to see. But the idea is the USB support makes this a dynamic process. And you specifically configure the host and the virtual machine so that the virtual machine will be able to acquire any USB devices that appear once that virtual machine is already running. So it sort of makes the whole thing more dynamic and fluid, much as it normally is when you're just running USB devices on a host without virtual machines.

Leo: Does it decide based on which window is front-most? In other words, if the virtual machine is kind of in the background, does it still grab the USB?

Steve: You're able to configure the – I mean, there is a problem because you've got, like, sort of a resource contention problem. So...

Leo: Right. Because what if I put in a CD-ROM, and I want it to be for the Mac, but I've got Parallels running? Who gets it?

Steve: Yeah...

Leo: Same thing with a USB device.

Steve: You're able to configure that on a per-virtual-machine basis.

Leo: So it will always get it if I've turned it on to get it.

Steve: Correct.

Leo: Oh, that's interesting. I was hoping, and it seemed to be, that maybe it was just when it was front-most only, but I guess not.

Steve: Yeah, it is a problem.

Leo: But, you know, I mean, hey. You're still getting to run two operating systems at once.

Steve: Exactly.

Leo: Raphael Wolff in Warsaw, Indiana has become a Parallels fan. He writes: Holy sheetrock! Parallels is amazing. Parallels is a virtual machine that you recommended in your last episode. It's for Windows and Mac. How is Parallels different/similar than a bootable flash key? Ah, interesting.

Steve: Yeah.

Leo: Using PE Builder and FlashBoot, he's been able to create a bootable Windows flash key, and a DOS key, as well. Is it possible to take the image off the bootable flash key and run it through Parallels compression and make it even smaller?

Steve: Well, this was a great question because there are two different solutions. There is, of course, the idea of creating, as Raphael has, a thumb drive that boots Windows. The problem with that – well, first of all, that works. It's useful. It allows you to sort of boot your own system that you carry around with you, with whatever apps and things that you've got installed on it. The problem is you don't get containment. That bootable Windows would inherently be able to see all of the resources on the host drive that you've booted it to. So if the host drive were infected, it would – well, and it's sort of a bidirectional thing. The host drive would not be running. But if by mistake you ran something on the host drive that was malicious, it could reinfect your thumb drive. And if something were wrong with your thumb drive, it could infect the host. So you don't, in that scenario, get any containment, which is what virtual machines, one of the several benefits of using full-on virtual machine technology.

And his second question about using Parallels Compressor, yes, absolutely. You could take the image from the thumb drive, compress it using Parallels Compressor, which as I said, you know, I did some benchmarks of size. I mean, that compressor really squeezes things down. And then put that smaller image back on the thumb drive.

Leo: I was crying about the fact that Parallels Compressor wasn't available for the Mac until I found out – and I got a number of emails saying, oh, it's actually built into the Parallels version on the Mac. You don't have to buy it as a separate program.

Steve: Exactly.

Leo: I was dumb. I didn't know that. I also want to point out – and I learned this from Cali Lewis at GeekBrief TV, that there's a new program, she's going to demo it on Call For Help this month, called MojoPac. But I'd like you to take a look at it too, Steve. The idea is, it's a PC on your USB drive. So your applications are in there. It's hard to tell if it's sandboxed or not. But it's MojoPac.com. And that's why I wanted to get your...

Steve: Is it .com or .org?

Leo: .com.

Steve: Okay.

Leo: And the idea behind it is that you could put, on a USB device or an iPod, for instance, kind of everything that you use. And you're working exclusively in the MojoPac environment, so you don't have to install it. And apparently it's running, you know, your desktop and everything are running directly from the MojoPac.

Steve: So it sounds a little bit like a bootable Knoppix CD; right?

Leo: Yeah, but you don't boot from it. That's what the thing – and that's why the security might be an issue; right?

Steve: Oh, I see. Okay. Good. We have had a couple listeners mention it. In fact, when I was going through questions just this morning, pulling out these 12, I ran across it. And because I didn't have a chance to...

Leo: Well, it's brand new. It just came out of beta, like, today, so...

Steve: Oh, cool.

Leo: So I'm very curious to find out what its capabilities are. So I'm not going to commit you to this, but I think we might want to look at this down the road.

Steve: I agree.

Leo: Yeah. It's actually also used, or intended to be used, by gamers who can't install games at work, who want to bring their games with them.

Brian Heyliger, soon to be a father – congratulations, Brian – in Tampa, Florida wonders: I'm a network engineer with heavy skills in Cisco IP telephony, but not so much in security. I'm also a member of my local church – and, as he said, is soon to be a father. In preparation for being a father, I've been thinking about ideas on how I might protect my daughter – wow, he's starting early, she's not even born yet – from pornographic websites and predators in chat apps, et cetera. You've got a few years, Brian, I'll be honest with you. My question is in regard to protecting innocent eyes on the Internet. It is always something to think about, though, as a parent. I want to be able to teach non-savvy folks how to protect their children from obscenities on the Internet. I'd also like to give a class at my local church on how to protect your children from certain websites, maybe even block certain chat protocols or filter/log the chat content so parents can have a little more visibility into who their children are speaking to on the Internet. Do you have any recommendations on a hardware device or software application that will accomplish this? Hardware would be ideal as it would control the whole network. Software would be acceptable, as well. The more user-friendly, the better, because the people I'll be teaching this product to will be typical PC users at best.

Steve: I liked this for a couple of reasons. First of all, the first thing I would refer Brian to is our episode on the hosts file. We've received a ton of great feedback since that episode on just, I mean, the phenomenal difference people experienced when they just changed that one file to the galactically comprehensive file which we linked to from the show notes, that third icon, on our hosts file episode. Because the hosts file, of course, intercepts a huge array of known yucky domain names and prevents browsers from going there. So, I mean, it's so nice and such a simple solution because it works universally among all machines. All Internet-connected machines somewhere have a hosts file, which is generally easy to find, depending upon what platform you're on. And, you know, it's a zero-overhead, zero-footprint – it's something you could easily, for example, in his church mode he could just say, look, folks, you know, here's the specific instructions, depending upon what kind of computer you have. And it just does a tremendous job of keeping your machine from going to these bad places.

The second thing that, you know, because he was interested in looking at some sort of a hardware device, I wanted to sort of touch on the idea that you and I talked about yesterday, Leo, of maybe doing a special episode where I really take a look at what Astaro is offering. Many people have been sending us positive feedback about their own experiences, but I've not yet made time. You know, I mean, for us they've just been, you know, a supporter of the show for a long time. And I like the fact that there was a good synergistic connection because they're into security. But from the standpoint of a hardware device, what you really want is something which is managed, something where, you know, as new bad things come along, somebody is informing that hardware device of what's going on. And that's one of the things that the Astaro Gateway system does do for you. It's not something that I've looked at it, but it might be worth looking at. And again, we would let people know, of course, that, you know, I'm not making an endorsement of it, but this is what the thing does.

Leo: Yeah, we should certainly test it and show people what it does. That would be fun. We decided because Astaro was an advertiser that it would be probably something we'd do as a separate episode, not as one of the regular episodes, just to avoid any appearance of conflict of interest. It's not something Astaro has asked us to do, but something we thought we'd like to do. But, you know, it's always a little tricky when a company is a sponsor. We have to be careful about how we deliver the content.

Steve: Exactly. And in this case, I mean, I really feel that it is being listener driven because there's been a lot of feedback. And people are saying, hey, you know, I'm trying to use it, what do you think of it?

Leo: Right.

Steve: And at this point I don't think anything of it. So I ought to.

Leo: One other thing I'd like to say, another sponsor, but this is a sponsor of my radio show, is a company called Phantom Technologies. This I think might be really more appropriate for Brian's clientele, who are not – believe me, the Astaro Gateway is not for a novice, nor is messing with the hosts files. They make a hardware device called the iBoss that is a parental control device. And it is managed, but it's managed at their end. So just like their iPhantom, it trans- all of the data that are coming into your computer is going through their servers. Which is managed in the same way you would have a high-end Astaro managed server. And so but it's not cheap, it's 90, I think it's 90 bucks, and there's a monthly fee. A good solution for anybody who wants to control a large number of computers. I use it at home. So, and we have four or five computers. And it does all of the things that you'd want, including filtering out bad sites. It does not log chats. That's another task that...

Steve: A really separate issue.

Leo: Yeah, you could use software to do that. And I have used software to do that in the past. But, you know, I have some issues about spying on my kids because they're a little bit older. But I think that, you know, in the past we – it's good to have the chat logs because if there have been any questions, we can go back and look at them.

Steve: It's also worth mentioning, too, I mean, Brian could use these things, these solutions that are available today, over for the folks he wants to help at his church. But given that his daughter is not yet born...

Leo: He doesn't have to worry about it.

Steve: Well, and I guarantee you that nothing we're talking about today...

Leo: Yes.

Steve: ...will be relevant in ten years, or eight years, or five years even, when it starts to be a problem that, you know, she might be using the Internet.

Leo: I think for his audience – you're absolutely right. For his audience today, though, MyiBoss.com is something I would absolutely look at. I've been very happy with it. I use it, and I've recommended it to a number of friends. And it does exactly the job that he's asking for, except for, as I said, for the logging of the chats, and that's a separate software. And very – that's an easy thing to do.

Shawn Milochik of Reading – I'm sorry, Reading – Reading, Pennsylvania, warns of a nasty new eBay phishing attack. Well, I think there's more than a few of those. I just thought you might want to mention this on the show. There's a new, to me, phishing attack on eBay. I'm a seller with active auction listings. I received a standard email sent through eBay by another eBay member, legitimately via their contact system. This is the way potential buyers contact the seller with questions about the items they're considering purchasing. However, the content of the email asks me to confirm whether my item is the same as the item in the link they provide. Of course that link brings me to a fake eBay log-in screen. Although – where they collect your password and log-in. Although there's nothing new about linking to a fake log-in screen, I think this deserves mention for two reasons: The email comes from a legitimate and expected source, in this case eBay itself. And unlike most phishing scams, where many ask you to log into your bank account at a bank you don't use, there's a 100 percent chance here that the receiver is not only an eBay member, but one with auctions, greatly increasing the likelihood of success. Thanks for the great, as always, Security Now! podcast. I'm subscribed to the monthly donation program mostly to support this show. Thank you for your donation.

Steve: I liked this question because it brought me up a little short. You know, I use eBay. I've been purchasing some stuff recently. And eBay from time to time just expires your log-in. And even though you check the box of, you know, keep me logged in on this computer, and it will ask you to reauthenticate yourself.

Leo: Yeah. I think most sites will do that.

Steve: Well, and that's the problem, is I realized, I mean, conscious as I am of phishing issues, and anytime I'm going to a site where it says, hey, you know, provide some information, I right-click on the page and check the credentials to make sure that this is, you know, really a site that's got an SSL certificate that matches the URL where I think I am. I mean, I'm diligent about that. But I realized I could fall prey to this.

Leo: Yeah.

Steve: If I were poking around eBay, and I got a page following a link that said, oh, it's, you know, it's time for you to reauthenticate yourself, I might very well do that. So I just wanted to raise Shawn's point. I think he's right. This is a sneaky one, and it might get me.

Leo: There is a very simple rule, you know, and I recommend everybody follow it. In the past our rule was don't open email attachments. And it's oversimplified because there are some email attachments that are safe. The very simple rule is, do not click links in email. And the reason is in HTML email you can hide what the link really links to. And so somebody who's not really paying attention will click a link in an email, it'll draw them to a website that looks like a legitimate eBay site, but if they look closely they'll see it's not. That's how phishing works. But in all cases it requires you to click a link in email. Otherwise it's not going to do anything. So it's just a good habit to get out of clicking email links of any kind. And again, there are some safe ones. But it's hard to tell which are safe and which aren't. You agree, Steve?

Steve: Yeah, and in fact, you know, I think I misread that a little bit. I was assuming that all of this was happening on the eBay site. But you're right, I mean, his note says, you know, he receives an email from someone. And it's like, okay....

Leo: Yeah. They can't fake a link in an email in an eBay site.

Steve: Right. Right.

Leo: So again, it's clicking that link in the email that really gets you in deep doo-doo. Don't do it.

Matthew Bain of Atlanta, Georgia had some great thoughts: I'm in the process of helping my aunt learn how to use a new laptop she just purchased for a therapy practice. And by the way, just to cross back to that eBay thing, what we didn't say is, if at any time you're concerned about a site you're on, it's asking you for log information, you can always get the certificate for that site and verify that it's the site you thought it was.

Steve: Right.

Leo: We should mention that, too. Back to Matthew: I'm in the process of helping my aunt learn to use a new laptop she just purchased for a therapy practice. She asked me about how to keep her patient notes confidential and secure. She has actually, I believe, under HIPAA, a requirement to do so. I'm going to teach her how to use TrueCrypt to store all her documentation. I own a MacBook Pro, and I use Parallels for all my Windows XP needs. I was playing around with TrueCrypt on my Parallels VM to learn some of its features when it occurred to me one could have a completely secured, encrypted OS by using TrueCrypt and a VM simultaneously.

Steve: Aha.

Leo: Ohhh. If one were to be running Windows or Linux with TrueCrypt installed, they could mount an encrypted volume, then create a new VMware virtual machine on that volume and the entire virtual machine, including system files, drivers, applications, et cetera, be encrypted. Instead of just encrypting your personal files from prying eyes, you'd be protecting the whole system. Is this a practical solution or simply overkill? Would there be a downside to using these two great products in this fashion?

Steve: Well, I thought this was really clever and interesting. First of all, I wanted to compliment him and his aunt on making sure that her laptop data is kept confidential. There are so many stories. I mean, it's phenomenal, you know, people who read security lists are seeing this all the time. People's, I mean...

Leo: Government agencies.

Steve: Yes.

Leo: The Veterans Administration. I mean, serious people who should know better.

Steve: It's just unbelievable. I mean, even now, years after the early high-profile stories about laptops getting stolen, I think people just assume, oh, well, I'll keep mine right next to me, or this'll just be temporary. It's hard to understand what they're thinking when, you know, data that they don't own is on a laptop which is inherently portable. And...

Leo: It's easy enough to secure it. They absolutely – it's crazy.

Steve: Yes, all...

Leo: We see stories, there were just stories this week about more government laptops missing.

Steve: Yup. All the technology is there. TrueCrypt is perfect for doing this. So again, I wanted just to salute Matthew and his aunt for, like, from the start they're going to solve this problem using TrueCrypt. And for people who are thinking about this and may now know what TrueCrypt is, Leo and I covered this in an earlier episode called "TrueCrypt." By all means, go back and take a look at it. It's just a – it's a fantastic solution.

As for the idea of using TrueCrypt to encrypt an entire virtual machine, it would work. But I'm a little nervous about the overhead. What TrueCrypt does is it is on-the-fly encryption and decryption, so that it's basically a filter which inserts itself between your operating system and a specific file or volume on your hard drive. So that any data being written runs through encryption as it's going to the drive and then runs through decryption as it's coming back. So the computer always sees the data as if it's never been encrypted. The drive always sees it always encrypted. So you're super safe because nothing that's decrypted is ever written onto the drive. So it's a beautiful solution. But that bidirectional process of encrypting and decrypting on the fly will introduce some overhead. So I would say, first of all, if you really want to do this, I mean, it's a great solution. It will work. You could give it a try and see if it slows you down too much. It just – it might bog things down more than the benefit is worth. But it would work.

Leo: That episode, by the way, was Security Now! 41. So if you go to TWiT.tv/sn41, you can listen to it right there on this page. And I was just looking at a news article because we’re going to probably talk about this on TWiT at some point. According to the Commerce Department – actually, yeah, the Commerce Department – they’ve lost 1,137 laptop computers since 2001, most of them from the Census Bureau. So obviously a lot of personal information on there. One hopes they were using some sort of encryption to protect those laptops. But that, I mean, they just – they will go lost. I always do everything I can to protect the data on my laptop.

Steve: Yeah, Leo, the only thing that I can imagine that is apparently going to work is for really strict legislation to exist that holds the people who lose the data accountable, and then makes the threat of what could happen so onerous and expensive that people are going, oh, well, I guess I have to figure out this encryption stuff.

Leo: Well, well, it should just be part of the government build, for crying out loud. It should be automatic.

Steve: Right, exactly. The IT people, when they’re setting it up, ought to just do it without thinking twice.

Leo: And there should be no way to disable it. And I wouldn’t be surprised if – and we’ll hear from them, I’m sure, if they’re already doing something like that.

Steve: And then we can hope they don’t just write the password on the bottom.

Leo: You can’t solve that problem.

Steve: You’re never going to get around the human problem.

Leo: No. Kye Dorton of Niceville, Florida – can you believe there’s a place called Niceville?

Steve: I just loved that, Leo. When I saw that in the mail I thought, okay, you know, here we’ve got a bunch of dirt. We’re going to make a town. What should we call it? Let’s call it Niceville.

Leo: Let’s drain the swamp and call it Niceville. I’m only up to Episode 44. Well, he just heard the TrueCrypt episode. But I’ve made it through all those in under two weeks. Wow, that’s kind of...

Steve: That’s dedication.

Leo: ...a crash course in security. I hope to be caught up in less than a week. I heard the question about how can virus damage a CPU. Can something through Windows or the BIOS hijack ACPI – that’s the Advanced Computer Power Interface, something like that – and shut down the CPU fan and/or other system fans at a time of high utilization to cause damage?

Steve: That was...

Leo: I wonder why he's asking this question?

Steve: Well, it was interesting because, you know, the question did come up, could something, you know, damage your hardware? Now, when a CPU gets overheated, it doesn't die, it just hangs. You know, the typical scenario is, when transistors get too hot, they stop turning off completely. They end up letting some current leak through. That'll cause the processor to essentially just hang. It'll just, you know, you'll get a system lockup.

Leo: Right. We see it all the time. Yup, yup.

Steve: Exactly. So that's what happens when processors get overheated. They don't die. But hard drives do. Hard drives really don't like running too hot. And it's one thing, it's one of the things that I encountered a lot with SpinRite 6. SpinRite 6 continuously monitors the temperature of the drive, if the drive is reporting it. And it will stop itself to allow the drive to cool off if the drive starts running too hot. And it was surprising to me, early in the development, how many people were encountering this problem. Because what's happened is people are upgrading to 7200 RPM drives from 5400, which are drawing more power, are generating more heat. But they're sticking them into cases, they're sometimes adding them to existing cases. And the cases are inadequate to keep all of that extra power cool. So, I mean, it's conceivable that if something came along and could take over your fans, which are under software control, and caused them to slow down, that you could create some permanent damage over the long term in your hard drives. But your CPUs, all they would do is lock up. And you'd begin to get the sense pretty quickly that something has gone wrong here.

Leo: Yeah. You know, you can – and there have been viruses that have written to the CMOS, changing the BIOS. So absolutely. And the theory behind this could absolutely happen.

Steve: Yeah.

Leo: Although we find the virus authors these days are not interested in damaging the system.

Steve: Exactly.

Leo: That's the old school.

Steve: They want to use them.

Leo: They want to use them. They want to sneak on there, use it for forwarding spam or putting adware up. And so for that reason alone, that would be counterproductive. They don't want to crash your system.

Steve: Yup.

Leo: Joe Rodricks, who obviously has a GPS because he says he's located at 42.01697 North and 70.967345 West – did you figure out it was Massachusetts, or did he?

Steve: He did. And I thought, okay, I'm not sure you want to give, you know, your exact location...

Leo: Exactly, within a few feet.

Steve: ...to six decimal places. But he did, so it's okay.

Leo: Go see Joe.

Steve: Maybe it's a Starbucks somewhere in Massachusetts.

Leo: I hope so. I'm praying. What's the best way to go about setting up a file server on my network? I have an old PC I plan on turning into a NAS device. And then I figured, oh, hey, ho, why not make it externally available? What does he mean about – oh, he means, like, to the outside world?

Steve: Well, that's a good – that's a really good question. I didn't know what he meant either by "externally available." But I wanted to mention that I've had really good experience using Samba, SMB or Samba, on a Linux or FreeBSD system, and using that as a file server. So, for example, if he had – and he talks about it being an old machine. Well, Samba is very efficient on, you know, as is in general Linux and FreeBSD, you know, any of the BSD machines, using that as a file server. And then you could also, of course, use it as your gateway, run NAT or firewall or whatever so that you've got one machine which is your network interface to the world. And, you know, if he really did want to make his files externally available, he would have that choice then because that machine would be the interface to the Internet, where he could – and in fact Samba does have lots of security provisions for, you know, passwords and log-ins and restricting IP ranges where things could be accessed and so forth. So one machine could be a sort of a general purpose file server/Internet interface for his network. And all the machines in the network could then easily use just standard Windows filesharing in order to access those files.

Leo: And that's built in, by the way, to every version of Linux and BSD.

Steve: Yes, it is now.

Leo: Samba is just an automatic...

Steve: Well, and I have to say, too, that, you know, I've never been a big user of GUIs on these Linux machines.

Leo: Well, then, there's no need if you're doing a file server. I mean, who cares about the

GUI; right?

Steve: Well, exactly. But what's so cool is I do have FreeBSD servers at, you know, in our main facility at Level 3, and I've got one here on my own local gateway. I don't run GUIs on any of them because, you know, Linux and UNIX are generally sort of text file configurable. You know, you've got various, you know, RC files and INI files and various types of files to manage and configure the system, but they're just text files.

Well, Windows is a perfect GUI. I mean, Windows, you've got text files coming out your ears in Windows. So all I do is I use Samba on those UNIX machines, and then I can connect either locally or remotely to – and of course I've got obviously firewall filter, so nobody else can even see that I've got Windows filesharing available to only my IP ranges, which are fixed at each end, that are able to see each other. So I just, you know, I bring up my UNIX file directory tree on Windows Explorer and then use whatever editor I want, because Windows has great editors and a perfect GUI, to edit the text files. So Windows is my management platform for these UNIX machines.

Leo: Yeah, that's pretty common, too.

Steve: It really works wonderful.

Leo: It's kind of a cross-promotion here, but Jeremy Allison, the creator – one of the creators of Samba, the maintainer of the Samba project, is going to be on FLOSS Weekly in a couple of weeks. And since you said you like BSD, and I know you like VMware, there is a BSD-based NAS distro called FreeNAS. NAS stands for Network-Attached Storage. And so it's a very simple way to set up a NAS using FreeBSD, absolutely free. And VMware actually – it was one of the appliance winners in their Ultimate Appliance, Virtual Appliance Challenge. It won for Best Consumer NAS. So...

Steve: Cool. And I would think Joe wants to look at that.

Leo: Yeah, it's small. It's 32 megabytes. So you could put it on a USB key, you could put it on – actually what a lot of people do now is they put it on flash, and they actually have the flash boot the system. You don't even have a hard drive to boot the system. It boots into flash, and of course you have the hard drives are storage only.

Steve: Right.

Leo: It's a nice way to go.

Steve: Very cool.

Leo: So, yeah, I think a lot of people are doing this. I bought a NAS because I wanted the hardware, the RAID 5 hardware. But you can build one if you've got an old machine.

Brian Lawson writes from Joburg, South Africa: Cell phones can log onto the Internet. You can browse with the phone's Opera – browser or Opera Mini. But cell phones don't have firewalls. What's the security problem?

Steve: Yeah. I thought this was a great question.

Leo: It is, now. I'm scared. I didn't even think about that.

Steve: Yeah, and it is a security issue. Certainly we've already seen situations where cell phones have buffer overruns which are exploitable. You know, it is entirely predictable that, as they become a bigger target, as more people are using browsers through their cell phones – and you know, Leo, that's my big application. I have a Treo 700p that I love. And all I do is use it for reading news when I'm roaming around. It doesn't support JavaScript at this point. That is, the Blazer browser in the Treo does not support JavaScript. So that's sort of a good thing. And I'm using very simple, WAP-based websites which are just presenting small pages, and I'm mostly just reading text.

But we know over time that's going to change. That technology is going to mature. The cell phones are going to be more powerful. People are going to say, hey, you know, I want to be able to do anything on my cell phone browser that I can do on my workstation. So we know that Java's going to be, you know, added to it. And along with that are going to come all the same security problems we've been dealing with on our much more mature platforms. So, you know, just keep an eye on security. It's going to be important.

Leo: Yeah. Although, you know, I guess the good news is these are such low-powered devices right now that they're not really a particularly attractive target.

Steve: Right.

Leo: I mean, there's some personal data on it, but – let's see, that was Brian Lawson. This is Brian Voeller of Ashland, Oregon. He brought up another interesting point regarding patents: I was enjoying your discussion on Parallels in the last episode, 59, but I did not appreciate the idea that patents on saving the state of a virtual machine were keeping others from doing the same. This is a very, by the way, hot topic in the open source world is the idea of software patents, and a lot of people don't like them. This is the same concept as state saving in console videogame emulators for computers. Here's a Google search for posts before the filing data of that odious patent, #6496847.

Steve: I got a kick out of this because, first of all, we did answer another of Brian's questions earlier. But you know, Leo, you and I have talked about the issue of intellectual property rights. And I'm very uncomfortable about this whole issue of software patents. From, you know, as a developer...

Leo: And here you're a software developer. So, you know, you have potentially something to gain from these things.

Steve: Well, yes. Except that what I have found is that what the – the Patent Office is issuing patents that it should not.

Leo: That's the real problem, yeah.

Steve: And that's a problem because then you've got companies that basically have a license to fight each other. Some other company says, wait a minute, that patent should never have been issued. The company that has it says, oh, we love our patent, we're going to defend it. And, you know, and nobody wins but the attorneys.

Leo: Yeah.

Steve: You know, in this sort of fight. And from my standpoint, the line that's crossed is sort of this, I mean, it is understandably a grey, fuzzy line. But it's the question of is this engineering or is this an invention? And the language in the patent law, which I have read extensively because I've been really curious, like, you know, what's going on here, is it talks about a solution which would not be obvious to someone trained in the art. That is, and so the question of is this obvious or not. And what I find is that most of the time companies which are first into an area, they will, you know, they're solving problems and coming up with solutions. Well, for a company to come along later to encounter the same problem and come up with the same solution, I mean, okay, sure. We see often that things are being invented at the same time by people who never talk to each other. You know, and so, I mean, that almost argues for the fact that these are not inventions, this is engineering.

Leo: Right.

Steve: And so, you know, the idea being, okay, I'm a software engineer. Give me a problem, I will solve it. Did I invent something, or did I just engineer a solution? And so often what I'm seeing are patents being issued for, you know, the only answer to a problem, which is not an invention. It's just, you know, you went to school, you learned how this stuff works, and then someone pays you to solve these problems.

Leo: Right, right.

Steve: So, you know, it upsets me that what I think we're going to begin seeing – and this is already beginning to start – we're going to see an increasing problem with patents that have been issued over the last decade which are going to cause much more trouble than they have as companies begin to sort of run out of steam and have to start going to litigation in order to, you know, find more sources of revenue.

Leo: Yeah. Yeah, I mean, it's really become a real problem. And there's a real challenge to this in the European Union where they don't really have these kinds of things. Or they hadn't had software patents for a long time, and now they're starting to implement them. And it's a problem. It's too bad.

Steve: Well, and in fact...

Leo: We see a lot of companies formed just to fight – just to, you know, fight over patents.

Steve: Well, yeah. And there are companies that are just □all they do is acquire patents, and they're just big litigation firms.

Leo: Right.

Steve: The original theory was that software could not be patented because software was just mathematics. That was the argument that the courts decided a long time ago. And they said you cannot patent mathematics because it's nature. I mean, it's just – it's here. You know, it's all around us. It's not something which was invented. And then what happened was, the way people began to get around this was that they would describe a software invention in a hardware embodiment. They would actually design hardware which would do the same thing. So they would patent the hardware and say, well, but the hardware is not the preferred embodiment. The preferred embodiment is this little software over here that's what they really wanted to do. But they sort of wedged it in by initially designing hardware to do the same thing. And then over time, you know, the Patent Office just sort of got – I guess they got tired of these ridiculous arguments and said, okay, fine. If you just want to patent the software, we'll let you do it. And of course now people are patenting genetics.

Leo: Right.

Steve: They're like, you know, patenting, again, things that already exist in nature that they didn't create. They just found them and said, oh, we're going to get a patent on this gene. It's like...

Leo: It's out of control.

Steve: It's bad.

Leo: Really out of control.

Steve: It's bad.

Leo: Steve, we've run through all 12, and you've done a great job. I think it's time to give you a day off.

Steve: Well, we're going to have a week and a half off since we're recording this one early.

Leo: That's right.

Steve: But we'll be back for #61, in terms of listeners listening to this, one week from now.

Leo: Yes. Don't get confused by what Steve just said. We are going to be consistent every Thursday, as we usually are.

Steve: Yup.

Leo: Thank you, Steve. We want to thank the good folks at Astaro, too, who are our sponsors and our supporters and, as Steve mentioned, do a really cool product called the Astaro Security Gateway. It is, you know, something I use. I use the 120. And of course it’s something that big businesses and big companies also use. It is a very sophisticated device. But what’s nice is it’s based on open source software, and they’ve done it right. The sponsors of the show, Astaro Corp., have offered your small or medium business a special deal. If your business needs superior protection from spam, viruses, and hackers, as well as complete VPN capabilities, intrusion protection, content filtering, and of course an industrial strength firewall, all in the easy-to-use single high-performance appliance, they will give you a free trial, a free demo. You just contact Astaro at Astaro.com or call (877) 4AS-TARO, and you can schedule that free trial of the Astaro Security Gateway Appliance in your business, which is fantastic.

And of course, as always, and I really want to underscore this, non-business users could download the software version of ASG for home use at Astaro.com. So another good way to build a security server would be to just get an old PC, download the free software, put it on there, and then I think it’s something like 79 euros a year you can get the full – subscribe to the antispam, antivirus, and automatically updated firewall and so forth. Astaro.com.

Steve Gibson, we will see you next week.

Steve: Absolutely.

Leo: We don’t know what we’re going to talk about. It’ll be something fascinating, no doubt.

Steve: No doubt.

Leo: Have a wonderful...