SECURITY NOW!

Transcript of Episode #96

Listener Feedback Q&A #20

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-096.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-096-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 96 for June 14, 2007: Your questions, Steve’s answers, #20.

It’s time to talk security with our friend Steve Gibson, from his highly secure and unknown workplace somewhere in Southern California, tempest protected. Here he is, Steve Gibson. Hello, Steve.

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

Leo: This is a question-and-answer session, and we do love doing those.

Steve: This is our 20th question-and-answer session, and people - really, I get lots of good feedback from people. In fact, now they’re writing notes in saying, okay, this is for - and they’re, like, telling me which one they want to appear on. It’s like, uh, okay.

Leo: It doesn’t quite work like that. However, I bet there are a few people who want to appear on the next one, which will be Episode 100.

Steve: Ooh, yes. Oh, that’s right, that’s a Q&A.

Leo: Yeah, hmm, mod 4.

Steve: Gee, is 100 evenly divisible by 4?

Leo: Not if it's a leap year.

Steve: I think it is, yeah.

Leo: Anyway, let's get on here. I've got a PDF open that contains...

Steve: Well, I've got a couple mailbag pieces here.

Leo: Oh, good, all right. I didn't even know we did mailbags on the Q&A days. I thought we're already answering questions. But we have a mailbag. We might as well do our mailbag.

Steve: It's quick, it's just two things. Justin Alcorn of Cleveland Heights, Ohio writes - he had a number of neat points. He said, "A couple of quick points on your Fourth Factor episode. First, I'm glad you're covering these authentication issues. Too many people assume that a username and a password is two-factor authentication, including a government agency that lost a laptop and assured the public that it was secure because it was protected by two-factor authentication."

Leo: Oh, man.

Steve: Meaning the normal Windows log-on.

Leo: Oh, man. I hope that was not disinformation. I hope that was just ignorance. Or maybe not. Actually, which is worse?

Steve: It certainly sounded good. Then he says, "There is a wonderful add-on for Firefox called PasswordMaker. It allows you to use a single password, and it hashes your password and the domain name of the site you are currently on to create a unique, random-looking password for each site. Since the hash is created the same way every time, you can get your password from any computer with the browser, or use the online JavaScript version if you are on a different computer."

Leo: I use something similar from Zarate Labs, same exact idea.

Steve: Yup, and I like it. And for what it's worth, there is also an add-on for IE. They don't have screenshots of it. They've got screenshots of the Firefox version on PasswordMaker. But I just wanted to - I thought that was a cool thing, and I've heard about it, so I wanted to relay that from Justin, our listener.

Leo: That’s a good way to do it.

Steve: And then he says, "When talking about the PGP web of trust, there are two things you didn’t mention." Actually there’s a lot of things I didn’t mention because I was trying to keep it somewhat simple and maintainable. He says, "You can choose how much you trust each signatory of a certificate. If you know people who just sign anything presented to them, you can trust them only a little. If you know people who are very careful, you can trust them a lot." Then you can sum up the trusts of people who’ve signed a given certificate - I added that part for clarity - to determine if you trust the certificate of a new contact. "Also, when determining whether to sign someone’s key, you should verify the key fingerprint to make sure you’re signing the correct key and not one that was presented to you by a man in the middle." And of course he’s absolutely correct about all of that. So there was more complexity, a lot more, actually, to the whole mature implementation of the PGP web of trust, specifically this notion that you get different sort of point credits for who signed it and how much you trust them. You then can, like, create rules in your system that’ll automatically decide whether this is trustworthy enough or not.

Leo: Right, right, right.

Steve: And then Christopher Adams, also a Security Now! listener, he wrote, "We have Albuquerque’s largest Christian home school association meeting next week at the church I work for. And right on cue, the laptop that contains all the data for this event crashed." He says, "The backup was stored in the North Pole with Santa, where the Easter Bunny and the Keebler Elves are keeping it company."

Leo: What he’s saying is there’s no backup.

Steve: Either that, or when we went to look for it, we couldn’t find it.

Leo: Oh, boy.

Steve: So he says, "Now, there were no problems with the hard drive, just a problem with the power adapter. So we simply needed the data quickly so we could move on with our work. I popped the drive into a USB enclosure, and sure enough, the drive failed." And so he says, "I guess having the power abruptly cut on a regular basis was not good for the laptop drive." And actually I chose this one because this actually perfectly fits with one of the questions in the Q&A. So he says, "After fighting through numerous error performing in page operation errors and learning that the solution was to buy a new hard drive, I quickly put the hard drive in a desktop case via a nifty $5 adapter, along with a CD containing SpinRite. Four and a half hours later, the service of this 60-gig laptop drive had been refreshed, and it now worked perfectly."

Leo: Wow.

Steve: He said, "I’ve been anxiously awaiting a moment like this where SpinRite paid for itself, and am happy to say it was worth every penny. And we bought four copies for a site license," exclamation point.

Leo: Oh, that’s great.

Steve: So he had actually written this to Sales at GRC. And he said, "Thanks, everyone. I cannot describe how much this has helped us. And it is a great case study for when I propose a file server with RAID and a backup system, instead of relying on individual hard drives."

Leo: That’s what I like about you, Steve. You don’t mind reminding people that they wouldn’t need SpinRite if they would just back their stuff up.

Steve: Yeah, I mean, I’m happy to be the solution that saved them the one time they desperately needed it and to suggest, you know, I hope to be able to help them a second and a third and a fourth time, and of course we’ve got owners whose butts have been saved by SpinRite throughout, you know, its 20-year life. But really, for mission-critical stuff, you don’t want to rely on a single spindle because, as we continually prove, they’re just not safe enough.

Leo: Spindles die. Let us get to our questions, shall we? We have so many of them.

Steve: Our typical 12.

Leo: Our typical 12, starting with Mark Brown of Cumming, Georgia, who says: I listened to Episode 90 - that was the one we did on multifactor authentication, the first three factors. And I wanted to know how to check for the certificate when I’m going to my banking site to make sure I’m really on the correct site. So he’s in his browser. He’s gone to his banking site. How does he know?

Steve: Now, we’ve talked about this many times, but I don’t think this is something I could say often enough because I’ll tell you, Leo, I mean, you know me. I’m not running AV. I’ve behind NAT. I don’t do scripting. I guess my point is, you know, I’m security conscious, but I feel that I’m generally pretty safe.

Well, having said that, one of the things I always do when I find myself about to enter my credit card information somewhere is I first make sure I’ve got https, and that the browser thinks I’m secure. Then I right-click on the page, choose Properties, and then choose View Certificate to make sure that, I mean, just to verify that no new phishing scheme has come along which is spoofing this page. And I always do this on PayPal because, of course, the larger the target is, the more likely it is to be spoofed. And so I make sure that the certificate that I’m viewing for the site is https://www.paypal.com.

So you want to right-click on the page, then tell the browser, you know, look at the page properties, then click on View Certificate to see the certificate. Then the one other thing you want to do is look at the chain of trust, that is, look to see who signed that certificate. Because if it’s Boris Badenov that signed it, then the certificate means nothing. The certificate is only as useful as the entity that is vouching for it, specifically, you know, someone like Equifax or VeriSign or somebody who is a standard signing authority. If your own, for example, if your corporate - if you had a browser had a corporate certificate installed in it, then your corporate proxy could be decrypting your connection, looking at it, and then reencrypting it. And so that’s something you might want to know. So you want to make sure that your certificate, that is, the certificate of the site you’re presented with has been signed by an authority you trust and that you’ve got a certificate for that site. And that will verify you’re actually connected to where you think you are.

Leo: Now, it’s a little different, slightly but not significantly different, in Firefox. You still right-click. And by the way, you have to be at https; right? I mean, otherwise there won’t be a certificate.

Steve: Correct.

Leo: So I went to Amazon.com, and normally it’s http. I added the "s." Now I’m at https Amazon.com. I right-click on the page in Firefox, select Page Info, and then click the Security tab, and you can view the certificate from there. And it’s RSA Data Security. Are they okay?

Steve: I think we trust them, yes.

Leo: We trust them.

Steve: We trust them.

Leo: That’s who you get yours from; right? Or is it VeriSign?

Steve: I’ve always been using VeriSign. It’s like, eh, why not, I’ll stay with them.

Leo: Very good question, though. And I think it is well worth saying again and again.

Paul Dickson of Phoenix, Arizona is concerned about biometrics. He writes: I’m of the opinion that gathering biometric data for identification purposes should be illegal. It’s fine you have the data on your notebook locked with your fingerprint, but can you or your estate survive if the data becomes inaccessible? If you’re in an accident where you lost a body part, are you prepared to not being able to access the disk contents? Of course backups would help, but what about changes since the backup? Disk recovery is going to be extremely costly. Alternatively, if you’re separated from your notebook, no one would be able to access your data until you’re rejoined. Not even trusted family can help. I’ve been told by someone who no longer has fingerprints, it’s quite common for nurses to lose their fingerprints. The fingerprint scanner might - must be the caustic chemicals they’re using or something. The fingerprint scanner might not be very useful for them. Then there’s a problem of whether a replaced fingerprint scanner on your notebook will scan your finger in the same manner. Steve, raises some interesting questions. I’m not sure making it illegal is - I think that’s going a little far. But he makes some good points.

Steve: He really does. So I wanted to bring up - it brings up a couple things. First of all, for what it’s worth, the fingerprint scans, for example, that I use for my laptop is a convenience measure. If I’m unable to authenticate with my fingerprint, I can always fall back to a password.

Leo: Oh, it doesn’t eliminate the password.

Steve: Exactly. So basically, if my fingerprint matches what it expects, then it’s providing the password to the BIOS in order to unlock the machine and to unlock the hard drive. And on this note I wanted to mention that, when I was doing some research into this stuff a couple weeks ago, I discovered Hitachi has announced and will soon, if not already, they are shipping, I mean, the galactic perfect solution for laptop hard drives. It has bulk AES 256 encryption built in.

Leo: To the hard drive.

Steve: So that it's not just locking the hard drive. You have to give the hard drive, any time you power it on, the cryptographic key that it will then use for all communication with the magnetic surface. Which means, I mean, this is what you want. Which means that all the data on the hard drive is always encrypted, not just locked, but a lock in the hard drive's own BIOS, where you could have a data recovery company get past that and then access it. I mean, we're talking strength that is absolutely transparent. They're doing bulk encryption that does not slow down the drive at all. That is, it's on-the-fly encryption to the surface. I mean, this is exactly what you want. Then, if you lose control of your laptop, it's like, well, that's too bad, but at least nobody can get to the data.

Leo: But what about Paul's point that nobody can get to the data? What if something happens to you, and your family needs to see the data?

Steve: Well, for example, in the first place, you know, when for example I authenticated a number of my fingers, just in case, if something did happen to one of them, to my right hand, I can authenticate with the other. And being me, you know, I sort of alternate consciously just to make sure that both of my index fingers stay happy. But again, in the worst case I've got a password. I don't want to, because as you know I've got a super strong password, so I'm not going to be typing that in easily all the time. And in fact, because my fingerprint can help me type in my super strong password, I was able to use a much stronger password than I would normally have bothered to. So but again, you could certainly - you could answer Paul's concern just by knowing that you always have the password as your backstop for your fingerprint.

Leo: I think he didn't know that. So that's good to know. I didn't know that.

Steve: Yup. And that was the point I wanted to make. That and to remind - I forgot to mention this Hitachi drive, and I've been wanting to because, oh baby, I mean, that'll end up being standard equipment on laptop drives before long, and it really provides us with the security that we need.

Leo: Yeah, interesting. John Everett writes from Virginia: I just finished listening to your SQL Injection Security Now! podcast. When you get to the point about how a hacker could get an improperly configured machine to divulge a list of all usernames and associated passwords, I had to write and ask, do people really stand up production websites that record passwords in plaintext?

Steve: Uh-huh.

Leo: I'm no security expert, but I thought the days of a passwd file - these are the UNIX passwords, p-a-s-s-w-d file - or equivalent were long gone. Isn't it standard practice now to hash the password plus some salt into a key that's stored? They call these encrypted password hashes. So even if a hacker got a list of usernames and the keys, that wouldn't be of immediate use because you can't enter the key directly into the website. Maybe you were glossing over this aspect in the podcast? In any case, I heartily agree with you, SQL injection remains a frightening vulnerability on the web. You were giving that as a example. It's not the only thing you can do with SQL injection.

Steve: Well, correct. But the point I wanted to make, the reason I brought this up, was that the insecurity is not only in the SQL injection problem, but in exactly what he says. That is to say, when he talks about there are well-known ways to do this right, he's absolutely correct. It doesn't mean that random Joe PHP programmer who just bought "PHP for Dummies," and it turns out that book is unfortunately correctly named in his case...

Leo: Aptly named.

Steve: ...it doesn't mean he is going to do it right because he's the coder. He can do anything he wants. He can store them in a text file and look them up, you know, have the passwords in plaintext. And so this is the message that I want to remind people of. It is incumbent upon the developer to implement security. The nature of Web 2.0 stuff is that this is a responsibility of the developer, and there are no requirements. Nothing in the language suggests it. If you have a developer who isn't aware of storing hashed passwords and then comparing the hashes rather than the passwords, which does create exactly the enhanced security that John's talking about, you have a programmer who just doesn't know about that, then you're not going to have it.

Leo: So, yes, it's just one more area of insecurity. Thomas Brock of Santa Monica wonders: As both a longtime SpinRite user and an employee of a large computer security company, I really enjoy listening to you and Leo. I have used and developed for Windows machines since Windows 2, 386 edition. I purchased my first Mac about a year ago. I really like it. One thing I've never wrapped my head around, though, is the Keychain. Every time I get a "Something wants to access your blah blah keychain," I always click Allow because I don't know what's going on. Could you please explain the Mac OS X Keychain?

Steve: And Leo, this one is for you.

Leo: Oh, thanks. No warning. Well, I think Keychain is actually one of the nicest features of OS X. It is a secure store of your passwords. When you use Safari on the web, it stores the passwords in this secure store. The store is unlocked by default when you log in. If the Keychain has the same password credential that you use when you log in, it will automatically unlock the Keychain. So that's nice. You can change the Keychain password or, conversely, change your master log-in password to your account, and then you'll have to provide a separate log-in to open up the Keychain.

But what he's talking about is a second layer of security, which I think is a very valuable layer of security. When you change a program, a program hasn't been used before with Keychain, when you update the program or reinstall it, the first time it tries to access the Keychain, and this is one of the reasons the Mac is more secure, the Mac says this program wants to access the Keychain, is it okay to do so? So just as with all of these alerts, Windows, too, with UAC, you've got to pause when you see that message and say, hmm, why is the Keychain being accessed, who's doing it, and does it make sense? So if you - and by the way, most Mac programs do use Keychain. Any program that has a password, for instance, like Safari, will use Keychain.

So here's kind of what happens. You updated Safari using, you know, Apple Update, and you use it. The first time you launch Safari, it says Safari wants to access the Keychain, is this okay? Now you think, well, I just updated Safari. I used Safari. Safari used Keychain. Yeah, okay, go ahead. And I think that's the point on all of these alerts is you've got to think about who's asking for permission.

Steve: Yup, in fact it's funny, you and I were talking before we began recording that I just updated my Skype from 2.0 something or other to 2.6 something or other. And sure enough, I got exactly this dialogue saying, hey, Skype wants to access the Keychain, do you want to give it permission to do so, now and in the future? And it's like, okay, yup, I know why it's asking, so let's go ahead.

Leo: And you can safely say no, in which case Skype won't provide your password for you automatically.

Steve: Right.

Leo: So I think, you know, this is actually kind of a response to your previous question. Apple has, I think, done passwords right. They don't store passwords in clear text on the drive. They store it in a secured store that is highly secure, using strong encryption, and that's what this Keychain facility is. And it's a very useful facility. There's a lot of features in there people don't know about. It will generate secure passwords for you automatically, automatically store them. It's like a password utility, the kind you'd go out and buy, but it's built into OS X. I think Keychain is really cool. Where you get into trouble is where you've changed your password on your master log-in or you move a keychain from one system to another. Then people get annoyed by it because it keeps asking for a password. You can also change the default behavior. Normally Keychain will stay logged in the entire time you're logged into your system. But you can change that. You can say after 30 minutes ask again.

Steve: Oh, very nice.

Leo: Probably not a bad idea to do that.

Steve: Well, and clearly the OS X also has a Keychain API that the applications are aware of and are able to access. And Windows has nothing like that.

Leo: No, I think this is a great idea. If you open - it's in the Utility, Applications Utilities folder, Keychain Access. You can see all the programs that use Keychain and what they're storing in there.

Steve: Very nice.

Leo: And that's where you would also change your preferences. And they have a First Aid and so forth. You can clear the log. You can synchronize the log-in password. There's a lot of Keychain settings you can change, as well. I think this is really great. It uses certificates; it uses standards. This is an example of where Apple has done things right. And, as a result, this is one of the things I think that makes OS X more secure.

Steve: Well, I would say that Thomas Brock got a beautiful answer to his question.

Leo: Well, good. I made it up as I was going along. Bob G. of Auburn, Alabama is worried about the health of his DVR: In Q&A 19 you talked about how the drive in a TiVo constantly spins. More than that, it constantly writes.

Steve: Exactly, it's constantly recording.

Leo: Yeah. The DVR that Charter Cable uses is a Moxi box DVR, works similarly to a TiVo. It would have to. If it has the ability to pause live programming, that's how it does it. During the podcast you said something about how a user should be careful when turning off a DVR to reduce the impact on the drive. Because we have short power outages of 15 to 20 seconds in my area - oh, that's nice - I've gotten UPSes for my desktop PCs and network equipment. Should I get one for the DVR? I asked when it was installed and was told no.

Steve: Well, of course he was told no because, you know, people look at it and think of it as just sort of a consumer appliance. And so I put this in here when I ran across Bob's question because I'm - and I even defended it once because I think we had another listener who said, I really don't think it's recording all the time. Well, we demonstrated that it must be because it's storing 30 minutes, and the TiVo and other DVRs don't have nearly that much RAM. So it's got to be recording it on the hard drive.

Leo: Let me - I just want to point something out because I think this is really important. It is perfectly possible to hear a question like that and say, well, let me find out and go research it. But I like how you work. You used logic. You thought about it. And this is, I think, what distinguishes somebody like you from a rote computer expert. You understand kind of the rationality of this, and you're able to think about it and quite quickly say, oh, no, there's no way it could because this is how it would have to work. And I like that. I mean, we could verify it, and I know it's true because it's completely logical.

Steve: Yup, so he does want, I mean, if he's concerned about this, a UPS makes a lot of sense. These devices can survive, obviously, some power outages because there's no on/off switch on them. You plug them in, and they're just on, just like a cable box is pretty much on all the time. In fact, even when you turn your cable box off it's still showing you the time of day, and it's on inside. Because you know when you plug them in they take about five minutes to boot themselves up and loading their code from over the cable. So these things are going all the time. And we do know that if you suddenly power down a hard drive when it's in the middle of writing, it will destroy the sector or sectors that it's on top of. And that's going to give a little road bump at that point when it comes around.

Now, they're built to be tolerant of that. But over time this adds up. So I would say give yourself a UPS. And maybe, after you put it on a UPS, if you can - often these cable boxes have all kinds of security, funky triangular-headed screws and things. But of course I've opened mine up and modified them extensively. If you can, take the drive out and, well, unfortunately, I didn’t mean this to be a SpinRite commercial, but I don’t know of anything else other than SpinRite that would do the right thing, and that is, run it on SpinRite - maybe Bob already owns a copy of SpinRite, in which case definitely run it on SpinRite to clean the drive up after you put your DVR on a UPS, and you’ll be in good shape from there on.

Leo: You know, thinking about this, I would imagine that, and I don’t know for a fact, that DVRs would use a journaled file system.

Steve: They don’t. In fact...

Leo: They don’t?

Steve: ...I can only speak for the TiVo because I know TiVo cold, and it is a standard ext2...

Leo: It’s not using Reiser or something. Huh.

Steve: Yup, Linux file system. And it’s an old version, an old kernel of Linux, and a small one, not a big fancy one.

Leo: I remember. Now, ext3 and Reiser and other file systems are journaled. OS X is journaled. NTFS is journaled. This is a bonus question. Doesn’t that give you a little bit more reliability in cases like this?

Steve: Kinda. The problem is, all of these systems are trying to be error tolerant, but they’re relying on the drive to be the sole store of their state. What NTFS’s system, for example, guarantees is that the way it writes, the file system structure will be maintained, but not the data. And nothing can solve the problem that, when you pull the plug and power fails during writing the sector, that that sector cannot have a proper checksum at the end, and there may be some power glitch happening. So the system is not going to be happy about it when it reencounters that again. So NTFS, and in fact this is something people don’t understand, NTFS protects its structure, but not the users’ data. That’s not protected.

Leo: Right. So a journaled system writes the data out in a batch. Is that what it means to be journaled?

Steve: Yes, the idea being that it’s creating a journal of changes so that, if something happens, it’s able to roll back to a point where the hard drive and file system were in a consistent state. And it may then be able to roll forward from the journal, given if the journal is also being written to the hard drive, it can roll forward to recreate the transactions which may have been damaged during the problem that occurred while it was journaling.

Leo: So it’s more robust, but not impervious to problems.

Steve: Well, and again, nothing can solve the problem that power failure during a sector write will make a bad sector. It absolutely will. And then when the system encounters it again, the question is, what does it do?

Leo: Right.

Steve: And it happens to be that's one of the things that SpinRite fixes. It, like, fixes all the checksums on all the sectors on your drive.

Leo: Interesting. Now, of course when you're playing back stuff on a DVR, a bad sector here or there just means a glitch in the video. It's not the end of the world.

Steve: It's not. But of course they're cumulative. And here in Auburn, Alabama, where Bob says he gets power outages constantly, it will add up. And I believe he'll end up seeing some problems. On the other hand, he can just tell his cable company, hey, this thing went bad, give me another one.

Leo: He's only renting it.

Steve: Exactly.

Leo: Lars Solberg listens in Norway. He's been comparing podcast advice. He's a bit confused by some apparent discrepancies. Well, we're always right, so I'm just going to say that right now.

Steve: When in doubt, ask.

Leo: I'm a long-time listener of the Security Now! podcast. I also listen to a bunch of other podcasts. One of them started talking about data backup and how long-time archival data can be safe on a hard drive that was turned off, just sitting in a closet or a safe. So I thought, well, I already know this, Mr. Gibson already told me, right? But they said on one of Norwegians' biggest IT podcasts that a hard disk drive is going to live longer if you keep the power on than if you use it as a backup solution. I clearly remember you and Leo talked about this, but I've been searching and reading through the text versions, I can't find it. Have I been dreaming? Can you clarify? How long will a powered-off hard drive live?

Steve: That's a great question, and I think what's happened is Lars got a little tripped up in some detail of what we're talking about, which is why I thought this was a great question because, Leo, I actually get a huge number of people wanting to talk about backup solutions. And it's something I've been avoiding because we're Security Now!, and I don't want to be too much pandering to SpinRite and backup stuff. But at some point we're going to have to do a show on hard drive backup solutions because it's a question that we're getting all the time.

In this case, the danger that a hard drive has - okay. First I'll just say we're both right. The major Norwegian biggest IT podcast is right and we were right because what neither or us were talking about is power cycling. That's the danger for hard drives is turning them off and on and off and on and off and on. I work to minimize the power cycling on all of my computers, where if I know, for example, that I'm not going to be using a computer for several days, then I'll turn it off. But I will never turn a machine off if I know that I'm going to be back on it in another hour because it's the thermal heating and cooling, heating and cooling, power on/power off, power on/power off that's the problem.

So I presume the guys who did the Norwegian podcast were talking about keeping a drive running all the time being better than powering it on and off. That's absolutely true. I was talking about putting the drive on the shelf, which obviously keeps it powered off all the time. And that's better than powering it on and off. So either extreme - all the time running, like the drives at Level 3 on GRC servers are on all the time, or all the time off - much better than power cycling constantly.

Leo: The heating and cooling is bad for them.

Steve: It really is.

Leo: Now, if you - and I know a lot of people do this. In fact, a lot of video production facilities, because hard drives are cheap and big, will just put data on them, they'll wrap them up in bubble wrap and throw them in the closet. Do you have to worry about things like stiction, bearings kind of getting gooey, things like that, if they're not used for a long period of time?

Steve: Well, decades maybe. I mean, but for really, really good archival storage, all the studies show that hard drives will last a long time, but also recordable DVD, recordable media - in fact, I bought a bunch the other day. It was an archive-grade DVD that is a gold - it's, you know, gold gold. It will only record at 1X. It won't let itself be recorded any faster than that. And it is built for 100-year storage and, you know, made very stable. So certainly decades, I think, are safe. I've got old original v1 IDE drives that I use for testing new versions of SpinRite. And I don't dust them off very often, but they still fire up when I use them. So problems like stiction, I think, have been largely solved. And taking a drive and just putting it on a shelf for many, many years is the best thing you can do for it. It'll still be there when you plug it in again. As long as you still have an interface that's compatible with...

Leo: Exactly. I think really the truth is, in the case of backup, no backup lasts forever. And as you point out, no medium will always be readable. So probably the prudent thing to do, if you do have something you want to keep a hundred years, is every decade or even more often you want to copy it to a more modern medium.

Steve: Yup, because, for example, try to find an ESDI controller.

Leo: Yeah, yeah.

Steve: You know, that was something that didn't last very long.

Leo: The heck with ESDI. Try to find a SCSI controller these days.

Steve: Right.

Leo: I mean, it doesn't take long. You got some stuff on ZIP disks, good luck. Orb? Good luck. I mean, that's the problem with this stuff is it changes. A decade is probably even too long. Maybe every five years. Then you refresh the data, you make sure it's good, you put it on something that's more modern that you can read. And I would guess, as time goes by, these archival solutions get better and better, too.

Steve: And of course the point is, if this stuff, if this data is really that important, then you do need to be aware of it and to give it the attention it deserves if it's that important.

Leo: Most stuff isn't. I can't - not much of what I do is worth saving a hundred years.

Steve: You know, and I've got - I have original - I have drives that I've pulled from old machines, carefully labeled, you know, here's 1988, my C drive. It's like, you know, maybe a walk down Nostalgia Lane would be interesting. But it's clearly nothing I need on that drive.

Leo: Your msdos.sys file.

Steve: Well, remember the days when we actually knew what all those files were, Leo.

Leo: Wow, look at that, it's an autoexec.bat file. Bruce in Gilbert, Arizona worries about sticky fingers. He says: Steve, I have a question on the security of a fingerprint scanner on a laptop. You state it's all you use to protect your laptop for log-in and to decrypt your drive for it to boot up. I've read that these scanners are pretty easy to fool with a copy of a person's fingerprint. Somebody did a test, you could make it out of Play-Doh, and it worked pretty well. I've read that these scanners - oh, we just said that. Would it be easy to get the person's fingerprint from a lost or stolen laptop merely by dusting it for prints? Sounds like a "CSI" episode. Your fingerprints would be all over it from handling it. You can also tell which finger is which by the prints left on the keyboard home keys, if that made any difference. Interesting idea. What do you think, Steve?

Steve: There are two classes of fingerprint scanner. The scanners which have a large, rectangular array, where you push your fingerprint against it, are inherently insecure for exactly that reason. You can make a Xerox, a static Xerox copy from an image and push that on the scanner, and it'll go, wow, this guy's got a high-contrast thumb. But it'll work. What I like, the only fingerprint scanners I trust, are the dynamic ones, not static, where they have either a two- or four-pixel-high optical array. And actually they're not even optical. They're actually capacitive. The...

Leo: Really...

Steve: ...fingerprint, yes, the fingerprint scanners that you see now on laptops that are that little strip that you...

Leo: It's just a bar, yes.

Steve: Yeah, the little bar that you wipe your finger across, they are not optical, they're capacitive. They work on the same principle as those stud finders, you know, those yellow stud fingers, you scan them across the wall, and it's able to tell when the density behind the wall increases. That uses a capacitive technology, which is the same thing that these dynamic fingerprint scanners use. So, for example, you could not swipe a Xerox of the image over the scanner. You actually have to have a 3D creation of the fingerprint. So not only does it have to be 3D, but it's got to be dynamic. You've got to move it across this scanner. And so using this several pixels' worth of - I'm sorry, I keep saying "pixel." Well, I guess they are pixels. They're not optical scanner pixels, they're capacitive scanner pixels. So using that strip, it's able to track the motion, seeing the image move from one row to the next. So it knows how far and how fast your finger is moving, but it's not using light, it's using the differences in capacitive reactance in your finger, which is much harder to fool. So not only dynamic, but capacitive. And that's a pretty secure way to pick up a fingerprint.

Leo: Fascinating. Alex Banks, writing from Los Angeles, asks: Back in Episode 68 - 68, wow - Q&A, a listener wanted to know about dual quad-core Intel processors. You and Leo commented this is probably overkill and that dual dual-cores were sufficient. What about heavy VM applications? These are the virtual machines that we've talked so much about, things like Parallels and VMware. Would the additional processing power greatly enhance VM performance?

Steve: Well, this is an interesting question from a couple points. First of all, the big load in VM is RAM because virtual machines essentially have to just take a chunk of RAM out of the hosting system and commit it to their own OS. That is, when you're running, for example, Parallels on a Mac, and you're running Windows, there isn't a practical means for Windows to share the main system memory in its virtual machine with the host's memory. It has to have all whatever it is, 512 megs or a gig or whatever. So heavy VM uses, that is, where you've got multiple VMs, they're all going to be grabbing a static chunk of memory from the main system. So really memory is the problem there.

Now, having said that, of course the more processors you have the better. Except that what you quickly run into is resource starvation in other places than processing power. For example, you can end up where, as I said, you don't have enough memory, or you can't get enough access to the hard drive because you've got processors that are doing so much, suddenly they're not the bottleneck. So as in any examination of a system, it's always the weakest link or the biggest bottleneck that causes the problem.

Leo: And often that's I/O. I mean, frequently that's I/O.

Steve: Yes, that's exactly the direction I was going to go in this. When we were being DDoS'd, being hit with Distributed Denial of Service attacks, you know, six or seven years ago, I did some study of what it would take to build a system that could respond to that. And it turned out that the PCI bus was instantly bottlenecked, that is, I couldn't get, no matter what fast code I wrote in the processor, no matter how fast the processor was or how many of them I had, I could not get a useful amount of bandwidth across the PCI bus to the network adapter. The PCI bus was the problem. So again, at some point you just end up with too much engine and not enough wheel.

Leo: I like that. I love that, in fact. Now, you used to drive, so you know what that means - too much engine and not enough wheel. I don't know what it means, but I like it. I have to say I have a quad-core Mac Pro, run Parallels all the time, runs swiftly, beautifully on that. And I don't think having an eight-core, which is what he's talking about, the dual quads, I don't know if an eight-core would make much of a difference, frankly.

Steve: Well, I built a machine not long ago that I think I've referred to here. I did get myself a quad-core Pentium. And boy is it fast for compressing media. Oh, my goodness, I mean, it'll spoil you in a heartbeat. I mean, as long as you've got a media compression technology that understands multiple cores and multiple threads, it's just shocking how fast it is because there you are massively compute-bound. Of course, now I'm going to get a call from the SETI@home guys, who are going to say, c'mon, get your screensaver going, Gibson, we want to use those quad cores to find the aliens.

Leo: Well, that's what they found with the PlayStation 3s, which have these new cell processors. And effectively I think they have eight or nine cores. They really do very well with these distributed computing applications. They rack up CPU cycles fast.

Steve: Well, in fact I've been messing around with AVID Liquid 7, doing some DVD production for my homeowners association. And many of the special effects systems, that software itself requires that you use a powerful video card because what they're doing is they're now offloading a lot of this work into the GPU, the graphics processing unit, because our graphics systems have become so powerful now.

Leo: And I run all the time a little CPU meter in my menu. It's a Mac program called Menu Meters. And I rarely, I have to say, peg it. But it is when you do things like rendering, transcoding video, things like that, where it really is processor intensive. It's hard, though, to get four processors pegged. I have to say, 2.something gigahertz processors, that's a lot of processing power.

Continuing on, Mike in Long Island has been experiencing email grief: My ISP provides email via POP and SMTP, as most do. However, they've caused much grief of late due to the following situation. The email addresses that my wife and I present to the world are in the form of myfirstname@lastname.net This domain is owned and maintained by my brother for various members of our extended family, as well as some of his customers. However, he's not in a position to provide storage, merely forwarding. Mail that goes to that address is then forwarded to the real address given to me by my ISP. The problem is my ISP seems to have some sort of antispam policy in place and appears to be bouncing some emails that are referred through this family domain. I'm very curious because I do the same thing. Evidently some sort of ham-fisted attempt to protect me. Well it's not ham-fisted. You're going to see more and more of it, actually. Worse still, they refuse to admit they're even doing so, making it impossible for me to convince them to whitelist this domain. I'm considering signing up with an email hosting service like FastMail and referring my emails there in the hopes of better results. Can you recommend any other courses of action? What's going on, Steve?

Steve: Well, it's exactly as you said, Leo. It is ISPs finally beginning to do what they can to minimize email abuse in the form of spam. The problem is, there is no good solution for him except to use an ISP that would be friendly to the idea of receiving this relayed mail. We've talked about before the SPF framework, which is becoming increasingly popular, or even Yahoo! uses domain keys. I think Google is able to use both. The idea being that you authenticate the server as the source of your email.

So the problem is, this guy is trying to send email from his ISP that has a different domain than the ISP. For example, if I were steve@cox.net, I would be using Cox's SMTP server to deposit my mail. It would then connect to another server somewhere and say, hi, I'm smtp.cox.net with mail from steve@cox.net. Well, due to this new antispam approach, the remote server would say, I really want to make sure that you're a qualified sender for email from cox.net. And Cox would say, yes, that's what I'm doing, I'm going to stand behind any cox.net email. Now, what Mike in Long Island is doing is he's sending email through Cox's server. So now when his email tries to go somewhere else, that somewhere else is saying, wait a minute, is this a valid source of mail?

Now, the good news is, I don’t know what his brother who’s providing this forwarding service, what capabilities his brother has. But potentially, if this were a problem with SPF - SPF is a DNS-based authentication system. If his brother has control of the DNS for this hypothetical domain lastname.net, his brother could put an SPF record, add an SPF text record to the lastname.net domain, authorizing cox.net as a valid emitter of email for the lastname.net domain. So it’s very possible that this problem could get solved by essentially, at the lastname.net domain, adding some SPF records to allow, essentially to permit Cox to be a sender of this guy’s email.

Leo: Microsoft has a wizard that will create this SPF record that you add to your DNS. So if you want to know more about that, do a Google search for "sender ID framework record wizard" on Microsoft.com. And you could fill it out, and then it gives you this little snippet...

Steve: And you just drop it in your DNS.

Leo: Yeah. Of course you have to have access to the DNS to do this.

Steve: Right.

Leo: So, and this was - I never quite understood this. By the way, Microsoft describes this, actually has diagrams and stuff, at Microsoft.com/senderid. I never understood this. So which end - do both ends need this modified SPF record?

Steve: It’s the sender end that needs somebody to represent that it’s a valid sender. So, for example, when email is trying to go to a remote server, the remote server sees firstname@lastname.net. The remote server then asks for the text records of lastname.net to find out who lastname.net has authorized as an originator of outbound email.

Leo: So it would say cox.net, or whoever his cable provider is, as one of the authorized senders. See, I need to do that because I use leo@leoville.com, but it doesn’t come from leoville.com, it comes from other - and so actually what I do in the reply-to field is I use the real ISP address in the reply-to. Which sometimes confuses people because they say, well, what is this I’m sending it to?

Steve: Right, right. And in fact, I mean, the good news is that the SPF protocol is very rich. You’re able to give IP ranges. You can give network addresses. You can do comma-separated lists. You’re able to really specify in a very nice and rich fashion what set of machines on the Internet are allowed to be senders of email from your domain. And it’s really cool.

Leo: And really complicated. And one of these days I’m going to understand it, and I’m going to fix it. But meanwhile, if you don’t get email from me, it could be that’s why.

Steve: At least you tried, Leo.

Leo: At least I tried.

Steve: It just bounced around the 'Net a while.

Leo: Yeah, I mean, I am completely sympathetic with the ISPs. But so many of us now use this kind of forwarding technique. It's just I don't know what this - I don't know. We've got to find a way.

Del in Wyoming, Michigan - and if that's not confusing, maybe his question will be.

Steve: I know. Wait a minute, Wyoming, Michigan? And sure enough, there is a town with a state name in Michigan.

Leo: I've been hoping to hear some follow-up on eEye's Blink program, now that there's been a few weeks to test it out. Does it work as advertised? How much does Blink slow down a system, if at all? Any noticeable failings, or is more testing required?

Steve: I have to defer to you, Leo. I know that you had installed it for a while. I just haven't gotten around to it. And so I wanted, for Del and everyone else who's probably wondering the same thing, I wanted to say I don't know yet.

Leo: It's a lot like a firewall in the sense that, when it sees outbound traffic it doesn't know about, it asks for permission, so you get those pop-ups initially. I have done very limited testing on just one or two machines. Here's what I've found so far. It does seem to slow the machine down appreciably. As you would expect. It's doing a lot of security. It's doing a lot of stuff. It can be intrusive in the sense that it's a very strong firewall. So for instance, I was using a Synergy KVM system that uses Ethernet to pass a mouse back and forth between two different systems. That of course was immediately blocked. And I had to go in and say, okay, no no, I want that port to be open. But it does seem, I mean - now, here's the problem. And I'm not equipped, and I don't know if you are, to test how well it provides security. I'm just saying, I didn't get any bugs while I was using it. But there are suites, you know, leak test suites and so forth - you do one, I know, Steve - there's other ways to test these things against viruses and against attacks and against leaks, and I haven't done that, so I don't know.

Steve: Well, I do know from looking at some of the feedback in the GRC Security Now! forum - which I will again commend to our listeners. You need to have a newsgroup reader configured to news.grc.com to get there. But it's a fantastic newsgroup. I mean, I depend upon it for sort of a real dynamic real-time feedback from the group of people who both listen to this podcast and hang out on our newsgroup server. They immediately jumped on Blink. And there were, you know, I've had good reports and bad reports. There was someone who complained that Blink didn't like the protocol that his newsgroup reader was using. Some of the packets were being flagged as potentially hostile by Blink. So there was an instance of a false positive. Some people did notice a performance hit. Others, whether there was one or not, didn't notice or complain.

So, and there was one problem, and that is that apparently in some independent analyses Blink did not fare well in the classic leak test tests because it's really not trying to compete in that category. You know, it's working to prevent bad stuff from getting in, rather than trying to, after something gets in, create containment for something that gets in. So the leak tests that are checking it for, like, cross-process vulnerabilities and code injection exploits, there are programs that will do a much better job of that because that's what they're trying to protect against. Whereas Blink is saying, you know, we're going to protect you from unknown vulnerabilities. And the bad news is, that's a hard thing to test. I mean, I know that the eEye guys have a suite of junk that they blast at their machines. Typical users don’t. So it is hard to independently verify it, exactly as you said, Leo.

Leo: Yeah, the tests you’re talking about I think are from Matousec.com. And they rated Blink very poor, along with a lot of well-known firewall programs, including ZoneAlarm Free, and say that the free Comodo is the best anti-leak protection.

Steve: And unfortunately what has happened is, Comodo, while it’s the best, it has been written to be the best.

Leo: Right. It’s designed for leak tests.

Steve: Exactly. They went in, and they deliberately fixed every type of exploit that was being tested for. So it doesn’t really mean anything except that it’s the best solution for leak tests. It doesn’t say anything about what would happen if a bad packet, an exploit, came in through a protocol that you were deliberately allowing and took over your machine. That’s what Blink blocks. And as far as I know, nothing else does.

Leo: Yeah, that’s difficult. It’s so hard to test security applications. It’s just really tough. And I don’t even attempt to do it. I would say my impression of Blink is, if you have a relative who you really want to lock this person down, maybe it’s a teenager who uses filesharing software, maybe it’s your mom who’s just not that sophisticated, and they can tolerate a little bit of slowdown, Blink is probably the best way to just kind of lock their machine down.

Steve: Well, and given its track record, which I think is proven, where it is preemptively blocking things months, I mean, many months, not quite years, but chunks of years, in advance of their being fixed, I think it’s still valuable protection.

Leo: Brandon, writing from an undisclosed location, asks: A few weeks ago I remember hearing an episode that talked about a program that would show hard drive usage by program, but I can’t remember the name. Do you remember what that was?

Steve: I really do, and it’s something I rely upon. It’s free. It’s called SpaceMonger. He wants the free version, which is v1.4. It got up to v1.4, and then Sean, the program’s author, decided, okay, I’m going to start again, I’m going to really do an amazing one, which is not free, it’s v2.something or other. I find that the free 1.4 is everything I need. What I love about it is that it gives you a graphical map of your hard drive, where you can see, using a series of nested rectangles, where your hard drive space went. You know, it’s like, wait a minute, I have a 120-gig drive, and now I’ve only got 10 gig free. Where did it go? And so with this thing you instantly see, for example, those nine DVDs at 4.7 gigs each that you ripped onto your hard drive and then forgot about, because they’re sitting there occupying a huge rectangular chunk of your screen. And you go, oh, and right-click on it and delete them right there. So it’s a very cool tool, and it’s free, and I just love it. SpaceMonger.com. Or I think it’s SpaceMonger in Google...

Leo: It’s called Old SpaceMonger. That’s the 1.4.

Steve: Right. And I'm sure he wishes I weren't telling everyone, it's all they need. But unfortunately he wrote a really good one before he tried to obsolete it. And it just works beautifully, and it's free.

Leo: There are a number of other programs that do this kind of thing. In fact, there's an open source one on SourceForge. I'm trying to remember the name of it.

Steve: Yeah. But Leo, I don't like it.

Leo: Oh, you tried it.

Steve: I tried to use - it's not nearly as nice. Yeah, it just, it doesn't - I was using something called DiskMapper from the guy who originally created Instant Recall, I think that was the tool. It was something, it was an old DOS app I was using as my general repository of all information, really cool tool. And he came out with it with DiskMapper, which I purchased years ago. But it really hasn't kept up. And again, this thing is free, and it just works perfectly.

Leo: SpaceMonger. And there are equal programs on OS X, as well, as a matter of fact, but I don't remember their names, either. Somebody called the radio show, and I've been trying to find them every since. A number of people emailed them, and now I've forgotten again. So anyway, but you've got one, SpaceMonger.

Jeff B., being irradiated by his city somewhere in Tennessee, writes this long but terrific note: I'm wondering what you guys think about the ever-growing implementation of public WiFi...

Steve: Thus the irradiation that he...

Leo: I get it now - both by cafes and such, as well as entire cities. I keep hearing about places that are putting it up for the public to use, but I rarely see anyone talk about the security or lack thereof. Well, you must not be listening to our show.

Steve: Except of course here.

Leo: Yeah, or my radio show, or any of the other - that just plain bugs me, to be honest. Worst yet, it's almost like some places try to cover up the security implications just to make the whole thing look better. Case in point, my town is implementing a citywide WiFi access. My town is doing the same, as a matter of fact. It's been boasted about on the news and newspaper as a great way to attract more businesses to the area and such. I think that's true. Sounds like flawed logic, but whatever.

Anyway, I got tired of the total lack of the security aspect being covered, and I responded to a story about it on the local newspaper's website in the comments section, pointing out some of the implications to not being particularly careful when on public WiFi, ways to protect yourself. I was careful to sound polite and helpful. But despite other comments showing up, mine never did. Only ones praising it ever appeared. People are thinking and being fed that it's just the best thing since sliced bread, who then think it's fine to go and do everything they do at home over it, having no idea that all normal traffic can be snooped in general, along with more directed methods such as ARP poisoning, SSL man-in-the-middle attacks, et cetera, et cetera. Even various folks that think they're being careful by not doing things such as banking don't realize that every time they load a page they're throwing cookies out at every http request to a site. Depending on the site, that makes it incredibly easy then to hijack their accounts.

Also - shall I go on? - also they pointed out in the paper that this city WiFi isn't made to replace their home Internet, in one sentence toward the bottom of the article. But you know as well as I do, as soon as people can pick it up from their homes they'll drop their cable/DSL in a heartbeat. I don't know if I have a point to this message, other than expressing my utter dismay at the lack of protecting people's privacy. But obviously it's not just a local problem, and it's only going to get worse as more places think it's a great idea to slap some WiFi repeaters up around town in an effort to make themselves seem more technological or whatever nonsense. The end. Signed, Jeff P.

Steve: Yeah. We're not sure where he is, but he's probably out on a sidewalk somewhere in Tennessee.

Leo: He has a good point. I mean, certainly we talk about it a lot. I probably talk about it every other show on the radio show because that's really the best platform I have for getting information out about securing yourself in WiFi. I mean, the radio show is listened to by a much more general audience than this is. If you listen to Security Now!, we don't have to tell you about this stuff.

Steve: Yeah, and I guess it must be the case that any really public WiFi system that is spread like that, there's no protocol for security; right? It's an all open system. And unfortunately, unless the users use VPN tunneling in order to tunnel themselves through a secure tunnel out of the wireless domain onto a wired backbone, which then goes to the Internet, everything they do is wide open. And, you know, his point about grabbing http session cookies is really a good one because it's so easy to hijack someone's session if the server is relying on a cookie to identify them. And those are, unless they're over an SSL connection to the website, those are in the clear and, I mean, easily sniffable.

Leo: Right. And then you could use it to have a pass- his password could be there...

Steve: Well, and just imagine the horror stories we're going to start hearing after this becomes widespread, Leo. And, you know, people are just sitting there, sucking in public traffic, you know, everywhere in a city, and going to town.

Leo: Although I know that a number of these providers are looking, and I'm not sure how it works, but they're looking at ways to make these things more secure.

Steve: Well, I've had a T-Mobile account for a couple months now. And I have to say I was very impressed. First of all, I was obviously very skeptical when I went to the whole notion of a public WiFi, public hotspot. But they do nothing but full WPA encryption. That is, you cannot set it up open. You cannot use it with WEP. They have their own little client, and it is WPA. So...

Leo: But that's a paid service.

Steve: Yes, it is.

Leo: And that's the key there. And if you're going to do an open hotspot, which is what municipal WiFi frequently is, that is inherently insecure unless they've come up with something to make it more secure, but I don't know - I mean, I read about this everywhere. We talk about it all the time. I don't think the message gets out to most people. I don't know, it's a very - it's an interesting question.

Steve: Yeah, I mean, the only thing I could see that would be practical, because we know now that WEP is so badly broken that it takes a minute to crack, would be some - well, actually there isn't a good solution because, even if everyone had a WPA key, if it was the same WPA key, you would just log in and be able to decrypt all the traffic then. So you would need enterprise-class WPA where you're doing per-client passwords so that no two clients on the same access point are using the same key. But now you're talking a seriously expensive infrastructure.

Leo: Yeah. I don't know what you do. I think really the word does need to get out. And maybe free or inexpensive WiFi security has to be made available, you know, VPN has to be made available if a city's going to do this, set up a VPN.

Steve: Yeah, but then again you've got people who won't bother. And, you know, if you let them get on the 'Net without security, I think we're going to maybe go through a period where there's a lot of pain and this gets a bad reputation before it finally gets fixed. Because, again, I think the barrier to entry for wide adoption has to be very low, or people won't use it. And very low means open.

Leo: It means insecure.

Steve: It means insecure, exactly.

Leo: Well, once again, with that we have come to the end of 12 good questions, and even better answers. You've done it again, Steverino. I don't know how you do it.

Steve: I chose the questions.

Leo: Oh, that's how.

Steve: I think that helped a little bit.

Leo: Yeah, that would have something to do with it. Well, I'm glad we did talk about all of these subjects. As usual, it's fascinating stuff. You learn so much. We'll do this again on our 100th episode.

Steve: Oh, and we're getting such great, great, great, great questions from our listeners. So I do want to continue to encourage people to go to the bottom of the page, the ever-lengthening long page, GRC.com/securitynow. Find your way to the bottom, and there's a form anyone can fill out. And unfortunately some bots are doing that now, too. So I have to...

Leo: Oh, man, I hate that.

Steve: So I'll have to do that, I'll have to fix something to stifle the bots.

Leo: Use a CAPTCHA or something. Every time you put a form online...

Steve: Well, actually that's going to be one of our future podcasts is titled, "Are You Human?"

Leo: Yeah, yeah. There's some interesting things going on to verify that. That's a huge problem.

Steve: Very cool thing.

Leo: Can you believe it, it'll be our 100th episode the next time we do this.

Steve: Yeah, very cool.

Leo: We're going to have to do something special.

Steve: Well, you know, I've been talking about having a special plan, but I'm a little worried about time getting away from me. I've been asked to keynote a conference at Harvard on spyware in a couple weeks, but the plan I had for the special 100th episode is going to take a lot of time, and other things have been burning up my time until then, so...

Leo: You know what, don't worry about it. We're not doing anything special for TWiT, either.

Steve: We'll get there.

Leo: We get these milestones. The milestone is, in and of itself, the success.

Steve: Well, it'll be fun to be there at 100 in four weeks, Leo.

Leo: We're going to beat you, though. TWiT's going to beat you.

Steve: [Grumbling].

Leo: I know, I know. You thought you might. It was a horserace. Well, who knows, anything could happen. It's not done yet.

Steve: How far behind are we, because...

Leo: You're four behind.

Steve: Ooh.

Leo: By the time this comes out - we're recording this a little early. By the time this comes out, TWiT will have done its hundred. Sorry. Sorry, Steve.

Steve: Ah, well, wait till we get to 200. We'll lap 'em.

Leo: All right. For more information about the things we talk about, and of course 16KB versions for the bandwidth-impaired - transcripts, too, for those who like to read along - you can go to GRC.com, that's Steve's website, where you'll find all sorts of information about Security Now!. That's GRC.com/securitynow. You'll also find ShieldsUP!, his great program to test - and his own LeakTest program, too - to test firewalls; all the great security programs he offers for free; and his bread and butter, the great SpinRite, the ultimate disk maintenance utility. GRC.com. Steve, have a great week. We'll see you next Thursday.

Steve: You know, Leo, you mentioned my own LeakTest utility. Mine is the dumbest one of them all.

Leo: And he's proud of it, folks.

Steve: It is so dumb, and it is the number one most downloaded thing I have. I mean, I'll come up with some new security thing, and for a couple weeks it'll be number one, and then it slips back right down. And LeakTest just sits there, just being - I don't know who's downloading it. But, I mean, it's so dumb.

Leo: Well, now you know why the people like Comodo and the other firewalls are tuning their firewalls to be resilient to leak tests. It's because of you.

Steve: People really do care, yeah.

Leo: There's something about leak tests, the people get it, and they want it. Whatever it is, I don't know what it does, but I want it.

Steve: Well, believe me, they've got it. Because, I mean, I don't even know what the count is now, but it's a phenomenal number of...

Leo: You should have charged for it, Steve.

Steve: A friend of mine said just get a dollar for each one. It's like, you don't understand the amount of overhead associated with getting a dollar. I mean, it's...

Leo: The transaction costs, exactly, yeah.

Steve: It's really substantial. In fact, it's funny, one piece of email that I read while I was preparing for this Q&A asked me a really interesting question that I think I might actually do a whole episode on. He said, you know, Steve, you've mentioned several times that you wrote your own ecommerce system from scratch. What are you most proud of and least proud of, that is, like, did you make any bad mistakes? And I did make one that's really kind of funny. And he said, and what are you most proud of? I thought, well, that's really an interesting question. But it wasn't something that I can cram into a few minutes, and I think people would find it interesting. So we'll probably - we'll do that one of these days.

Leo: I think that'd be a great subject. Let's do it. Well, I'm most proud of bringing hundreds of thousands of people to this show every week. I think it's a really great public service, and I thank you so much for doing it. We'll adjourn, but we'll be back, reconvene next week for more security information. Thank you, Steve.

Steve: Okay. And in the meantime, Leo - I'm not letting you go. In the meantime, I had the chance to bring up the download page. LeakTest has been downloaded 6 million, 6 hundred - more uses than ShieldsUP!. No, no, ShieldsUP! is 50 million.

Leo: 50 million, yeah.

Steve: But still...

Leo: Now, if you charged a buck you'd be doing okay.

Steve: 6,661,892 times. And about a thousand a day. Just mind-boggling.

Leo: Everybody who has used ShieldsUP!, just send Steve a dollar, will you?

Steve: No no no no no. Buy SpinRite because it'll...