SECURITY NOW!

Transcript of Episode #124

Listener Feedback Q&A #31

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-124.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-124-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 124 for December 27, 2007: Listener Questions #31. This show and the entire TWiT broadcast network is brought to you by donations from listeners like you. Thanks.

This is Security Now! with Steve Gibson, the post-Christmas, pre-New Year's edition. Leo Laporte here. Steve Gibson is in Irvine. And we should just say that we are not yet eggnogged out because we're recording this before Christmas.

Steve Gibson: Yes, we are. We wouldn't miss an episode, and we wouldn't leave our listeners hanging and saying, wait a minute.

Leo: You're amazing, Steve. And I'm in Egypt. That's the other reason.

Steve: You've made time for this, Leo, so I really appreciate that. And I know our listeners do.

Leo: Oh, no, yeah, no, you will now - I believe you will now have surpassed TWiT for the number of shows, at least after this one.

Steve: Finally.

Leo: Damn that Steve Gibson. Damn you. So we're going to do a Q&A this week, Listener Feedback #31. And we've got 12 great questions, including the official Duh! of the Week Award and the Fantastic Tip of the Week Award. I love that. Do you have any addenda, anything you want to handle before we get into the meat of the matter?

Steve: I did want to say at the beginning of the show something that I mentioned at the end of our show last week. And that is that I've had a number of people who have written in using the feedback form. I want to remind people about that as you always do, Leo, GRC.com/feedback, to allow people to send us their notes and thoughts. I get ideas for show topics and sort of some - it's an informal steering committee that I do pay attention to. A number of people have said, you know, the show is called Security Now!. Let's have a little bit more of the "now" in that. And they're right. We were probably a little better in our first year or two about talking about things that had happened that week, important things that came up. But I've gotten a little sort of out of focus on that. So my New Year's Resolution for the show is that in '08 and on we're going to - I'm going to be a little more focused on and maybe sort of add a little section at the top of each show about anything important that happened in the week in security news that we need to make sure our listeners are aware of.

Leo: But not this week because we're taping it ahead.

Steve: Exactly.

Leo: So we don't know what's happened. But nothing's happened, it's the week after Christmas. What could go wrong?

Steve: And we did have a listener, actually this is the one I noted, although a couple of people made a point of mentioning that I misstated the processor in the - remember we were in our little nostalgic phase a couple weeks ago. And I said that the chip in the original PC was the 8008, when in fact...

Leo: It was the 8088.

Steve: Exactly. The 8088 had sort of some 16-bit stuff in it. It was still largely...

Leo: It used a weird address space, as you well know, that weird extended address space.

Steve: Oh, as an Assembly language, yes, as an Assembly language programmer I found out about segmented address spaces. And I was really glad to go to a 32-bit flat address model when we finally got there.

Leo: Right about when that came out I was writing Assembly code for the 68000, which had a flat space.

Steve: Oh, and a much nicer chip, too.

Leo: It was a really elegant instruction set. It was very easy. My friend, Tim Pozar was writing Assembly code for the - we were both learning Assembly code at the same time. He was writing it for the X86, the 8088. And I've looked at the hoops he had to jump through to do memory addressing, and I thought, that is - because you have to rotate it over and, oh, it's just crazy. They had, what, a 20-bit, was it a 20-bit address space that they extended to make look 32? Or was it 24?

Steve: Good memory, Leo.

Leo: Was it 20?

Steve: No, it was 20-bit. Because in 16 bits you're able to access 64K. And that's where the 640K sort of came from was they added 4 bits, and then you were - so you're able to use those to access the total address space of the system.

Leo: Right. I apologize that Steve's quality all of a sudden - for some reason Adobe decided to download a 386-megabyte update to Photoshop. Stop it. Bad Adobe. Okay, it's stopped now. You'll sound better in a second. This is a problem, you know, with Skype, Skype sounds great if you have all the bandwidth dedicated to it. But as soon as - and computers nowadays, they're always doing something in the background, something without asking permission. So I think you'll sound better now. So it's an 8088.

Steve: It's an, yes, 8088 is the chip that was in that one. And then an 8086, no, I'm sorry, the 8286...

Leo: 80286, yeah. That was the AT.

Steve: That's what was in the PC AT, yeah. So correction in errata mode.

Leo: Hey, that was a long time ago. Come on. You can't expect us to remember all that. It's pretty amazing that we remember as much as we do.

Steve: If and when we do our old fart show with the old geezers, I'm sure there'll be all kinds of things where we're saying, wait a minute, like correcting each other in our aging.

Leo: That'll be fun. I'll have Wikipedia open as we do it, just to keep us honest. I thought you said 8088 because I wasn't listening closely enough. I mean, come on. But it's good to know we believe in getting things right. You got any great SpinRite - I bet you do - SpinRite stories?

Steve: What would make you think that?

Leo: I don't know, I just thought you might.

Steve: Okay, get this one, Leo. SpinRite aids hearing.

Leo: No, come on. Now you've gone over the top.

Steve: SpinRite helps you hear better. This one we received toward the end of November from a SpinRite user, Steve Nicholas, who said, "I'd just like to share a SpinRite success story with you guys. I'm a freelance IT consultant. And last week I got a call from a client of mine who's an audiologist. They have a dedicated PC link to some hearing testing and hearing aid programming equipment. This particular day they had switched on the PC, and Windows loaded, gave them an error about missing DLL, and then they had no desktops or any other option but to turn the PC off. Luckily this was a quiet day for them" - so to speak, the audiologists. Anyway, "This was a quiet day for them."

Leo: I get it.

Steve: "But they had lots of hearing assessments booked in for the following day. I looked at the PC and tried to start in Safe Mode, but still nothing worked. I then booted from a Windows XP CD and ran Check Disk. Alas, Check Disk reported that there were bad sectors on the drive and unrecoverable errors. I informed the client that they'd need to replace the hard drive and might possibly have to reinstall the OS and the apps from scratch. He looked even more worried and explained that he didn't have the CDs for the audiology software as it had been installed by the equipment manufacturer and was a nightmare to calibrate from a new install. I said I'd try my best and took the PC back to my workshop with the intention of cloning the partition to a new disk. But unfortunately the cloning software said there was a fatal error reading the drive. It was not looking good for the PC or my client.

"I then fired up SpinRite and left it running on the PC overnight. The following morning SpinRite had fixed the drive. And hey, presto, the PC booted up as normal. The BIOS SMART monitor said the drive was in danger of imminent failure, so I quickly cloned it onto a new disk and had my client's PC and audiometer equipment up and running by 9:00 a.m., and no appointments had to be canceled, and the practice could operate as normal, much to the relief of my client and his patients. Great work at GRC."

Leo: Yeah, that's a lifesaver. Wow. There you go.

Steve: So SpinRite does it again.

Leo: Got to keep, you know, we hear you, SpinRite, we hear you. So let's talk a little bit - actually, speaking of hearing you, we have listener feedback. Not that kind of feedback, feedback from our listeners. So let's get to our first call if you would like.

Steve: Absolutely.

Leo: Or first email, I guess. Stephan Buys in South Africa. He says - you say he scrutinizes every cookie: In the light of the recent privacy discussion, I wanted to offer the following advice - by the way, that was a great show. That was Episode 121, I believe, we talked about privacy.

Steve: "Is Privacy Dead," yes, right.

Leo: I wanted to offer the following advice regarding cookie management. Perhaps my approach is slightly over the top, but I found it does not impact my day-to-day surfing. See, that's my problem. You turn off cookies, and everything stops working. Apart from disabling and managing JavaScript using the Firefox NoScript plug-in, I've disabled all cookies in Firefox in preferences. You do this by unticking the "accept cookies from sites" box under the Privacy tab. Okay. You can then go to the exceptions button on the same page and manually enable cookies by site as you need them. I've explicitly enabled cookies for things like Audible where I choose to stay logged in, but most sites are blocked. So it's kind of similar to the NoScript, where you opt out unless you specifically, explicitly opt in.

Steve: Yeah. I liked his idea because I know that we've got listeners who really want control and who want to go even further than somebody who, for example, wants to just block third-party cookies. My normal practice is to allow first-party cookies but to disable third-party cookies. However, we've seen, for example, that there are still ways around that, such as we discussed in the PayPal/DoubleClick episode, where if PayPal hosted a link to DoubleClick that bounced you back to PayPal, then you'd be doing a first-party DoubleClick cookie. So what Stephan is talking about is, you know, goes further. And it would even block that sort of first-party cookie approach. So he's disabling even first-party cookies by default, and then he makes exceptions. As you said, Leo, he's opting into specific cookies that he wants to allow.

I'll mention that IE offers the same feature. That is, you are able to say I want to disable all cookies and then manually allow cookies only for specific sites. So if that fits people's way of operating, I wanted to make sure that they knew that was a possibility. You could allow MSN and Amazon and PayPal and explicitly the sites where you want to maintain an ongoing relationship with the site. You want to be able to stay logged on or be able to browse around. If the site is really broken, as frankly a lot of sites will be, then you can - but you say, okay, I care about this site, then you explicitly enable cookies only for that domain. And so the browser defaults to not ever sending cookies back even when it receives them, and only does so on the sites where you permit it. So again, it's a more restrictive policy, but it's going to be protection against even the first-party referrer approach that we described in the PayPal DoubleClick episode not too long ago.

Leo: The problem is, of course, knowing who to trust. And especially since, I mean, you'd think you'd trust PayPal. I guess I trust Amazon. But now what we've learned is more and more that these sites have deals with advertising companies like DoubleClick. And I don't know, can you?

Steve: In fact there was a blurb in the news a couple weeks ago, Leo, that sort of raised my hair a little bit. There's another company that is a major mail-order, physical world company that is talking also about combining that with online presence. That is, they're explicitly saying we're going to partner with people who are companies like PayPal, like Google perhaps, who do know your actual name and address, and who have given you cookies in order to match you up, to match your offline existence...

Leo: Ooh, that's really scary.

Steve: I know, it really is - to match your offline presence with your online presence in order to cross that boundary. And it's, I mean, it's something to be concerned about. And of course we've got Google purchasing DoubleClick that's one of the - well, in fact, DoubleClick apparently purchased a company some years ago that talked about doing this. And the outcry that came up ended up pushing them away from that practice because people were so upset with the idea of not only being tracked on the Internet anonymously, but making it non-anonymous.

Leo: Oh, boy. Well, let's hope - I think that awareness is so key. And as consumers do kick up, people, you know, nobody wants to make their customers angry. So there is some hope because when consumers kick up they do back off. We just have to stay aware of it, I think. That's really the key on this. So good suggestion, Stephen, or Stephan, I should say.

Ryan in Indiana had an interesting suggestion for WiFi security: I was listening to your podcast regarding using SSL, VPN, and SSH, one or the other, I guess, whilst traveling hotels and such, when needing to use a nonsecure network. My question is, while it's a great idea to use VPN to your home router while away, why not use VPN in your home to secure your wireless? It could be in lieu of or in conjunction with WPA, especially if you're using hardware or devices such as media extenders that don't support WPA. Would that - well, but if they don't support WPA, are they going to support VPNs?

Steve: Well, for example, we know that one of the show's sponsors, Astaro, offers SSL VPN, which tends to be the most compatible. We talked about this back in our early VPN episodes, that there were real problems with the traditional IPSec and PPTP protocols because they just weren't very flexible. But it absolutely is the case that this is - it's a workable idea. If for whatever reason your wireless did not support WPA, yet you had a router or some device that did support a VPN, and you're able to connect to it from your laptop, that is an absolutely rigorously secure connection which is proof against man-in-the-middle attacks of any sort, any kind of ARP sort of poisoning games. It's an absolutely workable solution for protecting your traffic. Somebody who was to hack, for example, your WEP key, or even leave your wireless open if you're not concerned about people connecting to your network by mistake, they would only see random noise packets going back and forth and would ever be able to get up to any mischief except that it, again, would be able to use your connection, which might or might not be a problem.

Leo: Oh, that's interesting. So that would be a way, if you wanted to open a connection up, that would be a way to do that. That's interesting.

Jeffrey in Columbia, Maryland has an idea about his system's hosts file. In past episodes we spoke about hosts files and how using it can limit your computer's exposure to some of the unwanted sites out there. Just to recap, you change your hosts file on your system, and you can block sites that way, point their IP address toward a localhost, for instance. So I was wondering, would entering your bank's URL and the IP it resolves to in the hosts file protect you from phishing attempts and/or man-in-the-middle attacks? That makes sense. So you have a BankofAmerica.com, and you hardwire it to their IP address.

Steve: Well, yeah. I mean, that is the idea, although I wanted to sort of clarify for Jeffrey and other users what the hosts file does. We've talked often about DNS, the Domain Name System, and how when you put in, for example, www.mybank.com, your computer goes out to the registered DNS server - typically that's offered by the ISP, it's running by the ISP - and asks that server if it happens to have a local copy of the IP address for www.mybank.com. If not, then it may resolve it for you. It'll go and find the current IP address for that and then end up returning that result to you. The hosts file is like a place your computer checks in before it makes an external query. So if you had in your hosts file www.mybank.com, and then the IP address that is the IP address for that domain, then one thing it is is faster because you're not having to go out and look it up. So there is a speed boost. However, most phishing attacks aren't trying to change the IP address associated with a domain name. They're, for example, misspelling it to mybank2.com, hoping that you're not going to notice that there's a numeral 2 after mybank.com.

Leo: So that's not going to fix it.

Steve: Exactly. So it would not prevent that kind of phishing attack. Now, I'm not sure what he means by man-in-the-middle. There are DNS man-in-the-middle attacks. So that, for example, if someone could infect the DNS system, and there are various types of DNS poisoning that have been done, then somebody could artificially change the IP returned for an external query to mybank.com and then end up intercepting anybody who was affected by that DNS poisoning and route them to essentially a hostile service and perform essentially a man-in-the-middle attack that way. So in that case, hardwiring the IP for your bank in your hosts file would prevent that kind of attack. The only other problem with doing so is that DNS can be used for load balancing. Major sites, for example AOL...

Leo: They change the DNS.

Steve: Exactly. Major sites like AOL will not have a single IP for AOL.com. They'll have a block of maybe, I mean, they may have a block of a hundred. But on any given query you'll typically have, like, five. And they'll rotate every time the query is made. The DNS server has logic in it which rotates that list so that there's a balancing effect. Everybody who asks for AOL.com has the IPs spread out among a number of different servers so that no one of them ends up carrying all the load. So if you were to hardwire one IP, then you would not get the benefit of that kind of load balancing. And of course the other problem is, if the bank's IP changed, you would suddenly find, because your hosts file would not be updating itself, you would think that your bank had gone offline. And in fact you'd be using the wrong IP for your bank if the DNS changed but your hosts file didn't.

So, I mean, it can give you a speed boost. It can prevent a DNS poisoning attack from succeeding. But on balance it's probably better to use it to block things you know are malicious. For example, we know that if you put DoubleClick.net into your hosts file and aimed it at 127.0.0.1, which is the so-called localhost IP, it will prevent your computer from ever having contact with the actual DoubleClick domain under all circumstances. So it's probably more useful to block things you know you want to block rather than trying to hardwire IPs for things that you want to prevent DNS from causing any problems from.

Leo: Good point. Very good point. It was a try.

Steve: Yeah.

Leo: Yeah. Anthony DiSante in New Tripoli, Pennsylvania likes pushing buttons: I love the podcast, and many of Leo's other podcasts, too. Thank you, Anthony. I purchased the PayPal football as soon as you guys mentioned it, and I feel much safer now that my account requires it, although I wish they didn't use the simple account number check as a fallback for when you don't have the football with you. I agree. That really obviates the whole thing. I also purchased the VeriSign VIP card when you brought it up. The card is so cool. However, I think I've discovered one big downside to it. You must use every number it generates in order, or else it gets out of sync with the PayPal server, which then starts rejecting its numbers. Now, I haven't found that to be the case, but...

Steve: I know.

Leo: Because the card is so cool, I've been showing it off to my friends, and naturally I'm pushing its button to generate a new number in order to show off the display technology. But apparently with the VIP you just can't do that. You can't throw away numbers as you can with a football and its time-based algorithm. Is this indeed the case?

Steve: Sort of yes and sort of no. I'm in the process of coming up to speed on the details of this. I have the documentation from VeriSign, and they've followed through now and created a formal evaluation account which will allow me to use these tokens in order to do validation. I'm hoping to get to that over the holidays. So probably by the time people are hearing this I may have been able to cross that bridge. But I have everything I need to from them, so I'm excited to spend some time doing this. The way VeriSign's back ends work, they're aware of people that might be pushing the button. I think that Anthony probably really likes to push the button.

Leo: Yeah, I haven't had any trouble at all. It seems to keep up fine. So it's not doing what the football did. The football generates based on - the number is based on timing; right? So...

Steve: Right. In the API there is absolutely a window. In the case of the football, that is based on time, you have a plus and minus window so that you can decide how far into the past or into the future, that is, how much desynchronization between the football's time-based token and the VeriSign servers are allowed. In the case of the credit card form factor, there's no backwards. There's only forwards. But so there is a window that says how far into the future of codes do you want to accept? How tolerant do you want to be of people like Anthony who are pushing his button all the time on the card and advancing the counter forward? And individual users of the VeriSign authentication system have the choice of how restrictive they want to be. So I'm not sure who he's authenticating with. But for example, if he's authenticating with PayPal, then it may be that PayPal has decided they want to be rather narrow and not allow, for example, more than 10 or 15 numbers ahead. Although certainly, once you resync yourself with PayPal...

Leo: Now, how do you resync? By having a correct entry?

Steve: Yes. I believe it's two in a row. That is, you give them one too far in the future, and they say, okay, we see you, give us the next one. And then by asking for two in a row that relocks them and proves that you have the card because you know not only this one but the immediate next one.

Leo: I see. Some people have said, oh, it's asked - and I've said it's happened to me - it's asked again after you enter it once. So that's what's going on, it's resyncing.

Steve: Yes. That's why the double request.

Leo: Okay. I guess I don't push it as much as Anthony does. I mean, I have. I play with it. But, well...

Steve: It's fun, yeah, yeah.

Leo: I don't play with it all the time. Chris in Los Gatos, California has been studying his RSA SecurID token. Is that the one we're talking about? Is that the same one?

Steve: No, no. Now, we've been talking about VeriSign, and RSA is very different.

Leo: They're a competitor. He says: I found an error with your comments about the RSA SecurID. It seems like the PayPal keys that you and many people have talked about are different than the ones I use at work. I work for a large aerospace company. I do mean large. Everyone's probably heard of the company; the initials are LM.

Steve: I think that might be Lockheed Martin.

Leo: Lockheed Martin? Or Leo's Machinery? I don't know. You have said that the PayPal keys have a sequential first digit, add one to the value of the first digit for the next key number. My RSA SecurID that I use for corporate VPN does not have any sequential digits, and there's no predictable pattern in any of the six digits that appear on my key. And as we know, that's a better thing. Does this mean I have more security than your PayPal key, since I have six digits of random numbers and yours only has five? Considering the company I work for, we have a very good reason to keep what we work on as secure as possible.

Steve: Well, I wanted - I'll correct Chris a little bit. He said that there's no predictable pattern in any of the six digits that appear on the key. I would say, well, there's no...

Leo: He can't predict it.

Steve: Exactly. There's no trivially predictable pattern. But it's certainly the case that it's based on a pseudorandom sequence which is absolutely predictable, although you need a crypto algorithm in order to figure out what they're going to be next. But he's right about his point that the so-called PayPal football, as we refer to it, the time-based token that those guys use does have, as we've discussed, the first digit increments sequentially, which is used as a shortcut, allowing the server to guess within a plus or minus couple minute window which key you're on.

Now, as to is it more or less secure, it's like, well, okay, I suppose - and as we've discussed also, that the fact that you've made one digit predictable then brings the challenge down from one in a million to one in a hundred thousand. On the other hand, it's changing every 60, I'm sorry, every 30 seconds. So the only reasonable attack would be some sort of brute force attack. But the target of the brute force attack changes every 30 seconds. And you're always authenticating about a back-end server. So the back-end server can say, wait a minute, this guy has just missed five attempts. We're going to lock him out. Or we're going to slow down our responses. Or we're going to wait on purpose for another 30-second window to pass by in order to prevent that kind of attack from happening. So I guess what I'm saying is that, yes, technically the PayPal football approach that has one predictable digit is one tenth as secure. However, it's already way more secure than it needs to be because it's being time based, and the target of any attack is changing every 30 seconds.

Leo: Yeah. But I can also see, I mean, so why - they do that so that - we talked about this in detail, I just forgot. Why do they put that sequential number in there? Makes it easier for it to sync up.

Steve: Exactly. Exactly. They have to do less work in order to check against codes. And in a heavy use environment, it's going to...

Leo: Save server, save server work.

Steve: Exactly.

Leo: Okay. And so Lockheed Martin has far fewer users, and so they can afford the server time.

Steve: Right.

Leo: Bob Thibodeau from Coral Springs, Florida is worried because he's got both WEP and WPA at the same time: During Episode 118 you guys discussed using a router that had both WEP and WPA available at the same time so that WEP-enabled devices can attach to the network. You seemed to indicate that this was a safe way to accommodate WEP-only devices. Actually I don't know if that's what we said. I can see that using WPA on my computers and WEP for my ReplayTV will keep my computer traffic from being sniffed. But doesn't the WEP hole in my network allow someone to get on my network and see any shares? And of course they would have access to my Internet connection. If they were able to get into some illicit trafficking, wouldn't I be liable? So I think you said that. I think that exactly was your point.

Steve: Yes. As we've discussed, due to the problem with ARP poisoning that we discussed some time ago, which allows somebody bad who had accessed your network to insert themselves, essentially create a man-in-the-middle and be able to filter any traffic coming and going from your Internet gateway, which is absolutely possible. That means that any access to your packet traffic is a problem. The only safe way that I can see to solve the problem is to have three routers. You would have your main router, which is your Internet connection. Then you would have a router running WEP and a router running WPA, both connected to that first router. So you essentially have a Y, and two routers running different WiFi. The reason this works is that you still have the potential for an ARP poisoning problem except that ARP will not cross a router. ARP is only used within a local Ethernet. So you end up with essentially three Ethernets. You've got an Ethernet on the inside of your WPA router, an Ethernet on the inside of your WEP router, and then you've got a little tiny Ethernet that's linking those three routers.

Well, that ends up being sacred, that little three-router Ethernet, because there's no way for anybody even who breaks your WEP security to mess around with the little network that links the routers. So essentially the routers provide isolation. But if you allowed WEP access to, for example, your main core router, the router on the outside, then it would be able, if that were hacked, to gain access to all your network traffic. So there's no way to do it that I've been able to think of with two routers. You would need three. But if you had three routers you would be able to use WEP services on one, WPA services on the other, and there's no way that even somebody with access to the WEP router would be able to gain access to any of your WPA traffic.

Leo: Okay. So it's somewhat more secure. At least they can't sniff you.

Steve: Yeah. Well, they can't sniff you. Now, on the other hand, you also have complete isolation between those two networks. There would also be - there would be no way for filesharing to work across them. So they would be completely isolated segments.

Leo: That makes sense, yeah. Ken Keating in North Carolina is taking no chances: Having become even more aware of cookies thanks to your recent episodes of Security Now!, I noticed that VeriSign's OpenID tool, when using Seatbelt in Firefox, creates a cookie, even when you don't log in. Wow, that's interesting. I have now disabled Seatbelt until I can figure out what state it thinks it deserves to save about me when I haven't even logged into OpenID.

Steve: Yeah. What's happening there is that Firefox, running as a plug-in, has web browser-level capabilities. So it's autonomously able to create a relationship with VeriSign's OpenID back end just to sort of be there and be present, even if you're not logged in. I've spoken to the guys at VeriSign. I've had a number of phone conversations with them, the techie guys in the back room and the more marketing-oriented people upfront. I just know they're on our side, and there's just no way that they're doing anything wrong with Seatbelt and Firefox. They really, I mean, they're pro users, they're pro security. They recognize that Seatbelt with Firefox really provides additional security for people who want to use OpenID. So I think the fact that it is creating a cookie is a completely benign side effect of the fact that it's a client of the browser running as a plug-in in the browser, and that it creating a cookie is just a fact that the VeriSign server is sending cookies back with the response traffic from Seatbelt, and the browser is just saying, okay, I'm going to store this cookie.

Leo: It makes the point that, yeah, we may not like cookies, but there's a lot of functionality they provide that's kind of needed. I mean, it's how you save state.

Steve: Exactly. It's certainly the case, and we've talked about this extensively, that cookies can be abused. But boy, are they handy.

Leo: Yeah. If cookies did not exist, we would have had to invent them. Mark in Fort Collins, Colorado wants his data really gone: I was using DBAN, says Mark, Darik's Boot And Nuke - that's a program I recommend all the time, dban.sourceforge.net - on a hard drive to wipe the drive before formatting and use it as a boot drive, and I was puzzled with the options given to me by the program. I've heard that writing zeroes to a drive, or zero-filling it, does not necessarily mean that the drive data is gone. In fact, it needs to be zero-filled several times to ensure the information is truly gone. But why? Why, why, why are three to five passes more effective than one pass when it comes to ones and zeroes on a hard drive platter? If a drive is zero-filled even just once, come on, how can information still be retrieved? But doing it three to five times makes it more unrecoverable? What's going on, Steve?

Steve: What's happening is that the magnetic impression that the hard drive's head makes on the ferrous surface of the disk is an additive process. So if you write, for example, zeroes on the drive, what you're actually doing is putting down a pattern of flux reversals...

Leo: Whoa.

Steve: ...in the magnetic surface of the platter. And you're writing them strongly so that, for example, when you come back around and read them, they're what you're going to read. But you're essentially, in putting down flux reversals, you are overwriting the pattern of flux reversals that was there before, but you're doing so in an additive way. That is to say that, if you were somebody doing forensic recovery, who didn't want to read what was last written on the drive, but instead what was written before what was last written, it would be possible to subtract out that last written major footprint on the drive and figure out what had been there before.

Leo: Really.

Steve: There is vestigial magnetism, that is, a vestigial pattern underneath what has most recently been written. The drive...

Leo: From a practical point of view, how hard is that to read?

Steve: Oh, it's tough. I mean, you have to be NSA sort of guys in serious data recovery, national security sort of mode. But it's been shown that that data can be recovered. And that's what Darik's Boot And Nuke is all about is that it is - and it's actually, Darik's Boot And Nuke is going a little overboard because current technology has evolved so far that even when you're writing zeroes on a hard drive, there's all kinds of things that make the actual pattern nonpredictable. And it's necessary that you have a predictability to understand how the flux reversals map back into the data. What drives are doing now, drives go through, like, four different levels of conversion to go from user data to final flux reversal timing in order to do all kinds of work, in order to allow them to get the density up to where it is today. So back in the old MFM and RLL days where we had 20 megabytes and 30 megabytes, this sort of data recovery was more practical. I would argue that, you know, probably writing zeroes is just fine. But if you've got time, and you really want the data gone, then writing more than once is a useful thing to do.

Leo: Simson Garfinkel, who was an MIT grad student who did a study of drives, he did an interesting thing. He bought a variety of used drives on eBay and a variety of places, got them from recycling centers, and studied them. Some huge percentage, it was like 80 percent, still had all the data on there. He got credit card numbers and all sorts of stuff. But I asked him when we were talking about - and this was a couple of years ago - if it was necessary to write over and over and over. He said, you know, no. He said overwrite them once is fine unless they've got some pretty - nobody's going to find it. And, you know, even in the NSA I wonder. But I guess if you're running from the federal government, okay. And it is the Department of Defense. I mean, this is a Department of Defense spec, this writing and erasing, writing and erasing.

Steve: Right. One of the things, actually it's an interesting little tidbit, if you were to write zeroes to your drive, then if you were a SpinRite owner and ran SpinRite on it, SpinRite reads and inverts the data and then rewrites it, reads it, reinverts it, and rewrites it. And remember it flips all the zeroes to ones and ones to zeroes and back again. And so it has the effect of pushing that history of what was on the drive back into the past further. So it's sort of a simple way of - you would need to zero it first, otherwise obviously you're going to end up with the same thing. But if you zeroed it first, then ran SpinRite on it, it would have the effect of doing that multi-pass, really push the data gone, gone, gone.

Leo: There you go.

Steve: There you go.

Leo: Matt in Ohio needs heavyweight encryption without any fluff. Steve, he says, I'm in need of securing/encrypting files at work on a shared network drive. I cannot install anything on the computers I frequent, or the server. This is pretty common in business. The department I'm in shares a single logon on several department machines. At most I can use a thumb drive. I would save everything to that except that, one, I need a backup, servers are backed up daily; and, two, there's too much to save on a thumb drive. Okay, well, I guess never mind. Is there something I can use where the software is loaded on a thumb drive and is used as the key to unlock files? In other words, he wants to encrypt on the hard drive, but using software running on the thumb drive.

Steve: Exactly. It turns out that most of the encryption tools around offer the benefit or the feature of integrating with the Windows Explorer context menus, meaning that they need to be installed, they're making changes to the registry, they're not just a simple little lightweight standalone tool. However, there is a really nice little lightweight standalone tool that I wanted to tell Matt about and tell all of our listeners about. I don't know what the name of this thing comes from, but it's called Omziff.

Leo: Well, at least you can Google it.

Steve: Exactly. If you put "Omziff" into Google, it'll find it for you. I've checked it out relatively thoroughly. It's not very big. It's about 400K, so it'll fit easily on the smallest of thumb drives. And it runs perfectly from a thumb drive. It uses state-of-the-art encryption. A whole bunch of different crypto algorithms are there. My favorite, Rijndael, is among them. And you're able to give it a password, and it will encrypt a drive. So, I mean, it just does - it's a very, very clean, simple, lightweight, standalone encryption system. And for example, if you just have one file that you are sensitive about and you want to encrypt, this is a perfect little tool for doing it. It just zips through it and encrypts it; and then you reverse the process, and it'll decrypt it.

Leo: Thank you for asking that question, Matt, that's really cool.

Steve: Omziff.

Leo: Omziff. So TruCrypt is too heavy to - it has to modify stuff to do that.

Steve: Oh, boy, yeah, it's - I mean, now you could install that on your thumb drive, but...

Leo: That's what I thought.

Steve: ...that wasn't what Matt was wanting to do. He was wanting, essentially, to encrypt a file and then store the encrypted file on his corporate server, and then take advantage of the fact that they're going to be backed up, the servers are going to be backing up an opaque blob that they're no longer able to read, and nobody in his company is going to be able to read it. So, I mean, for anybody, it allows you to just do a simple, standalone encryption of a file and then do anything with it you want to safely. It turns the file into, as we know, absolutely random noise. And the only way to get it back is by decrypting it with the same key.

Leo: Very nifty. Security Now! listener Tom in Buffalo, New York brings us this week's Protecting Users From Themselves even if they don't want it note. And boy, I agree with you, Tom, on this one. He's talking about Western Digital's new Anywhere Access. This is a - it's only on their terabyte network-attached storage drive they're doing this so far. And one hopes if everybody kicks up enough dust they'll drop the whole idea entirely. But this is some software that they've put on their network-attached storage drive, their terabyte drive, their MyBook, that prohibits what?

Steve: Well, yes. Cory Doctorow made a posting in Boing Boing that Tom referred me to. And I did a little research to find out what was going on. Get a load of this, Leo. They refuse, by filename extension, to allow certain files to be made available on this hard drive that they're saying - it's like a server that allows people to access it from anywhere, except if the file has an AAC or an AIF or an AVI or a CDA or a DVI or an MP3. You can't store MP3 files on your own hardware. This thing says no.

Leo: You can store it, you can't share it, I think is the...

Steve: Exactly, exactly. It will not allow you to access those. And I love it because...

Leo: Which means why store it because you can't access it.

Steve: Yes, exactly. In their own online facility they ask the question of themselves, what files cannot be shared by WD Anywhere Access? Answer: Due to the - get this - due to the unverifiable media license authentication, the following file types cannot be shared by different users using WD Anywhere Access. So they're...

Leo: Why would they do this? It's insane.

Steve: So they're saying, because these files tend to be...

Leo: We can't be sure you're not stealing, so we're not going to let you do it.

Steve: Yeah.

Leo: And who would buy this? The problem is that a lot of people buy it because it's not obvious that it's doing that till you get it home.

Steve: Yup. So I wanted to make sure - I loved Tom's question, and I wanted to make sure that all of our listeners knew that this was the case with WD Anywhere Access, that they were proactively, preemptively, and without anyone knowing it, saying no, we're not going to allow you to share these types of files, by file extension. I mean, which is dumb because all you have to do is change MP3 to MPE or something. Oh, sorry, no, that one is an MPEG video format. You can't use MPE either, or MPEG, or MPG.

Leo: To TMP. Oh, no, you can't do TMP files, either. Well, as a matter of fact, don't buy this stupid drive. Oh, this makes me mad. You know, it's not too late to have them win the Dumb Move of the Year Award. It comes towards the end of the year. But I think this is easily the dumbest thing I've heard all year. Unbelievable. Just bad for business. And boy, I feel sorry for anybody who's bought this thing. We'll put a link to the Boing Boing article so you can read this. And so far, as far as I can tell, it's only on one particular model of the MyBook. I bought a MyBook. I like the MyBook. I've been recommending the MyBook. This is those big Western Digital drives. But these new terabyte network-connected hard drives I'm never going to - and I have to say I don't think I'll buy anymore Western Digital products.

[http://www.boingboing.net/2007/12/06/western-digital-netw.html]

Steve: Nope.

Leo: No, don't think so. Why take a chance? Are you ready, Steve Gibson, for the Fantastic Tip of the Week Award? Josef Ender from Neuheim, Switzerland writes: In Episode 120 Brian Dewey asked for a possibility to download all the patches and fixes for Windows XP. c't, a great German magazine, created an offline update script for many MS systems. Oh, that's neat. And you'll find it at Heise Security, that's heise-security.co.uk.

Steve: Yes. People can just Google "offline-update" in order to find it quickly. This thing is so cool. When I learned about this from Josef, I grabbed a copy, downloaded it. It's a ZIP that you expand to a little directory. Basically it's an EXE. It's got a beautiful UI. You say, I want to build an ISO CD of all the updates from, like, from the beginning of Windows XP. And this thing uses Microsoft's own tools in order to access Microsoft's site. It downloads all the security patches. It downloaded Service Pack 2 and everything since, and ended up building a single 680-meg ISO which you could then burn to a CD, and you've got a single disk that brings any newly installed, freshly installed Windows XP right up to speed. Or Windows 2000, or Office 2000 and 2003, Office XP, I mean, it's completely multilingual. I mean, it is really cool.

A number of people responded to, as Josef did, to Brian Dewey's question because I had remembered that there was some way, somewhere on Microsoft where you could get a list of these things. A number of people talked about something called RyanVM, I think it was, but then bemoaned the fact that it hadn't been updated since June, which of course it's like, well, okay, you're a lot further along than you were with just Service Pack 2, so maybe you only had to install, you know, 50 patches instead of 95. But this thing, because it uses the realtime data directly from Microsoft's Windows Update site, it knows how to parse all of the metadata. It downloaded all the patches, merged them all together, and built one single ISO image. It's just extremely cool.

Leo: So I guess, you know, I had mentioned a system that worked in XP and within Windows Update of going to the network update, network updates, and seeing the list there. But this makes it so much simpler.

Steve: Well, yes. And if you're someone who's installing XP, I mean, the real question was...

Leo: Reboot, reboot, reboot, how long is this going to take, and have to do it over and over.

Steve: Well, and as I remember Brian's question, he did not want to be on the 'Net. And so my response was, well, now, as long as you've got Service Pack 2, if you've got Windows XP with Service Pack 2 you've got the firewall turned on by default. Even if you didn't have Service Pack 2 you could make sure your Windows firewall was on, and you're probably safe. But the beauty of this is this is an offline update. So you install Windows XP. You then use this CD, and it will bring you absolutely current with never going on the Internet. And this site is very nice, too, because it demonstrates the Microsoft Baseline Security Advisor, that BSA tool that's able to analyze the state of your machine, it shows a before and after where just by applying the CD that this system builds, the Baseline Security Advisor is completely satisfied. It says, okay, you are absolutely current. So this thing does it with no network connection.

Leo: But, well, it has to get an Internet connection initially to download everything; right?

Steve: Yes, yeah. So, exactly, so you would have a machine on the 'Net that you would use to build this ISO. But then it builds one, I mean, this is what I'm doing from now on, Leo. I just did a Windows install the other day. And it's like, oh, here we go, you know, reboot reboot reboot, download download download, blah blah blah. Now I've got this disk, it's what I will do after I install Windows XP, before I go any further. So even if you didn't build one of these immediately, until Service Pack 3 comes out for Windows XP, which we know is in beta somewhere, until that comes out, this brings you, like, up to now. And then you'd only have to do, you know, whatever patches had come out in the second Tuesday of the month cycles since then. So, I mean, it just brings you much closer.

Leo: Really cool. Again, just Google online - or I'm sorry, "offline-update." And it is the first item that shows up there. But it's from heise-security.de, and then click on the English flag to get to the UK site. And Karsten Violka and Torsten Wittrock are the two that worked on this. Really neat. That's a neat idea. That's the way to do it.

Steve: And I've got to tell you, the execution, I just think they did such a nice job.

Leo: Is it batch files? How are they doing it?

Steve: No. Well, it's an EXE and then a bunch of command scripts. And all of it's there. You can browse it, you can - I mean, I was thinking, hey, how did they make this ISO? Because, I mean, there it is, there's an ISO you can burn to CD. And they just - they did the whole job. It's trivial to use. It's a fantastic system.

Leo: And you pick the version. It actually works for Windows 2000, XP, and Server 2003. So you can pick your version.

Steve: And every language you ever heard of.

Leo: Really neat. Really neat.

Steve: Oh, and all the Office stuff, also.

Leo: Oh, really. Oh, great. So if anybody's got to build Windows systems, XP systems or 2000 systems, this is a must. It's a must. Thank you, Josef. Really good recommendation. And finally, the Tim Hoolihan from Akron, Ohio Duh! Award of the Week.

Steve: I read this, and it's like, uh, duh.

Leo: Duh. Several weeks ago you guys discussed a listener's logon encryption scheme. In discussing the JavaScript hashing encryption that this listener asked about, I believe Steve said it was sufficient, except that the session cookie could later be sniffed. Maybe I'm missing something about the system, but I think the system is still susceptible to sniffing problems during the logon process. My understanding is that a form provides a user and password field, and as the form's data is being submitted, some JavaScript does an elaborate process of three hashing systems with some salting values thrown in. This is described as a one-way process. You'd be correct to say that it would be tough - read impossible - to guess the password if you sniffed those values. However, I don't need the password. If the process is one way, then the server has the hashed version stored, and that's what's authenticated. For instance, user "bob" logs in with a password "spot." The resulting hashed password is, I don't know, X12345. If I sniff and see a form post with fields user:bob and pass:X12345, I could build a simple HTML form that posts those values to the same URL. I'd be authenticated and redirected to the same page as a valid user. Ooh, yeah.

Steve: You remember, we were talking about that guy...

Leo: He had that crazy scheme.

Steve: Well, yeah, he took the password, and he ran it through an MD5, and then he added some other stuff, some random stuff. At some point he got gobbledy-gook from GRC's Passwords page. He mixed that in, and then he did an SHA1 hash, and he went up, you know, I mean, really just hashed it to pieces and ended up with this no doubt, you know, bizarre output from either the MD5 hash or the SHA1. And we were all kind of, our eyes were crossed, it was like, oh my goodness, you're never going to figure out what that was. But he did it because he didn't want to use SSL. And so we ended up saying, yeah, well, that's really not a replacement for SSL. Well, the beauty of what Tim points out is that, if he's not encrypting the submission, then the result of all that, even though it is so distantly related from his original password that you could never get back to the password from that...

Leo: You don't need to because it's sent in the clear.

Steve: Exactly. So you've sniffed that. And it's like, okay, I don't know what the password was, and I don't...

Leo: Who cares?

Steve: I don't care.

Leo: Don't need it.

Steve: Duh.

Leo: Whoops.

Steve: Anyway, so Tim, you were absolutely right. You didn't miss anything. I should have picked up on that and mentioned it myself because it's the obvious weakness. Sure, you could catch the cookies going back and forth. But there's no need to do that. If you did catch the original submission, you could certainly logon in the same fashion anytime you wanted.

Leo: There you go. Just that simple. And that's why you need many eyes looking at security because nobody is perfect all the time. And that concludes our 12 fascinating questions from 12 brilliant listeners. If you'd like to submit a question for our next listener questions episode, you can go to Security Now!, the Security Now! website, which is GRC.com/feedback. Right?

Steve: Yup. That'll give you a form. And again, I want to encourage people to please give me ideas for shows they want to see, or hear; ideas for questions for our Q&A episodes; and just in general any sort of feedback. I get way more than I'm able to read, but I absolutely do read them. I respond when I can. And they do form the basis for our even-episode Q&As. So keep those questions and feedback coming.

Leo: Keep those cards and letters coming in, boys and girls. We really appreciate your listening to the show, everybody. We do remind you that you can get 16KB versions for the bandwidth-impaired at GRC.com, along with Elaine's great transcriptions, show notes and more, GRC.com/securitynow. And while you're there, make sure you check out SpinRite, everybody's favorite disk recovery utility, disk recovery and maintenance utility, really great program. Also Steve's freebies, like ShieldsUP and Perfect Paper Passwords and all that great stuff. The forums are there, too. It's really a good site: GRC.com.

And I understand, Scott Jordan at ScotteVest tells me they're going to extend the coupon code till the end of the year. So you have a couple more days if you want to get some great deals on ScotteVest. Maybe you were waiting for something under the tree and it didn't come. ScotteVest.com, use my name, LEO, as you check out, as the coupon code that'll knock 20 percent right off the top of the price. So and there's still lots of good stuff. In fact, they have some clearance deals and so forth. Everything on the site, 20 percent off when you use my name, LEO, as the coupon code. Steve, it's been a great year.

Steve: It's been a fantastic year. I wanted to thank our listeners for all the help and support that they have provided to us both...

Leo: You bet.

Steve: ...this year. And we're plowing into 2008. I'm going to work to honor my, as I've mentioned in the last couple weeks, my New Year's resolution is to add a little more of really current information about what happened during the week as a regular section in the podcast moving forward. And again, we won't be able to do that next week because we're recording that one tomorrow, many weeks in advance. But starting with the second one of 2008, that content will be there.

Leo: We're busy. Busy, busy, busy. Well, Steve, have a great New Years. And we'll see you in the New Year. This will be our, what, entering our third year of Security Now, or is it our fourth year of Security Now!?

Steve: Yeah, we're in our third. So we're at about three and a half, I guess, at this point.

Leo: Unbelievable. Wow, that's great. Well, thank you so much for a great show and a lot of great information. I feel like I'm a lot smarter about security and privacy and all those concerns since we started doing this. I really appreciate it. Happy New Year, buddy, and we'll see you in 2008.

Steve: Talk to you soon, my friend.