Listener Feedback #69

Description: Steve and Leo discuss the week's major security events and discuss questions and comments from listeners of previous episodes. They tie up loose ends, explore a wide range of topics that are too small to fill their own episode, clarify any confusion from previous installments, and present real world 'application notes' for any of the security technologies and issues we have previously discussed.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-202.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-202-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 202 for June 25, 2009: Your questions, Steve's answers, #69. This show is brought to you by listeners like you and your contributions. We couldn't do it without you. Thanks so much.

It's time for Security Now!, the show that covers all things secure. And ladies and gentlemen, the star of our show, Mr. Security himself, Steve Gibson. I can give you a Johnny Olson.

Steve Gibson: We also - yeah, you know, we just lost Ed McMahon the other day.

Leo: Yeah, isn't that sad.

Steve: Really sad, yeah. He lived, I think he was 86, and then he 86'd himself. So no one really talked about what the cause of death was. But of course you and I grew up with him and Johnny Carson.

Leo: Oh, he was so good. He was so great. I think it's interesting because I think you and I are of an age that Johnny and "The Tonight Show" was really important. I didn't realize Leno had done it for 10 years. So that's amazing.

Steve: Yeah.

Leo: And now he's moved on, and it's Conan O'Brien.

Steve: But you remember the big controversy when it was who's it going to be, Leno or Letterman.

Leo: Yeah, they made a wonderful miniseries about that.

Steve: Yeah, exactly.

Leo: That was really good. What was - I can't - was it called "Night Shift"? I can't remember. Anyway, hi.

Steve: Hello, Leo.

Leo: How are things going? First of all, I've got to ask you, how's your DX?

Steve: We have that question. The first question on the show actually is that because I had a note to bring it up last week, and I just - I hadn't written it down, and so I forgot in scanning my stuff. So let's do that when we get into our Q&A.

Leo: We'll save it for the questions. This is a Q&A day, as all our even episodes are.

Steve: Yup.

Leo: At least for the time being. And, good, so I want to find out about the Kindle DX. Before we get to our questions and answers, is there any security news to talk about?

Steve: Yeah. Not heavy news. There was, of course, mega news last week and the week before. I did want to mention that all Mozilla stuff - Firefox, Thunderbird, and SeaMonkey - have recently been upgraded to fix, naturally, some bad various sorts of remote code execution exploits. So Firefox needs to be at, as of this podcast, 3.0.11, where mine is. Thunderbird comes up to 2.0.0.22. And SeaMonkey needs to be at 1.1.17.

Leo: As of this recording.

Steve: As of this recording. This is all a moving target, of course. So but as of this point, that's where you want to have those versions.

Leo: Now, I'm using the beta of 3.5 on Firefox. And I don't know if they've updated that. I presume they have.

Steve: Yeah. I read something about that recently, I don't remember what now.

Leo: The release candidate one is - let me check. The last version that I got was release candidate one. Let's see if they have - I'll check and see if there's an update.

Steve: And as I remember, that adds some HTML 5 features.

Leo: Yes, that's where we're all headed. And I'm sure you're going to hate that.

Steve: I'm hating it.

Leo: [Laughing].

Steve: If it's new, I'm skeptical.

Leo: Yeah, it doesn't say "beta" anymore, so I guess this is the final 3.5. I'll check for updates and see if they're updating it. Nope, no updates.

Steve: Now, I did note that we - last week we commented on the release of Safari 4. And there was a little tweak that they made to it to version 4.0.1. Not a security issue, just a compatibility issue with iPhoto. So they fixed a little problem that they had. This sort of stuff, software development, sort of tends to mature and get finished exponentially, where the rate of things that are being fixed slows down, but it doesn't just stop instantly. So it makes sense with a big new release like this they would have found something that sort of sneaked through their final qualification.

And then I did want to note something that I just picked up in the news. We also talked about the iPhone having been updated to 3.0 and all the new features that it offers. I thought it was also significant that it fixed more than 46 security vulnerabilities.

Leo: Wow.

Steve: That existed in the last version 2.0 release in Safari and Mail. And that those flaws, which they kept relatively quiet about, could be exploited to make calls without user interaction, execute malicious code, and crash the phone. So, and also interestingly, that number of fixes is nearly four times as many as in the previous iPhone update. So they're focusing on it and keeping it clean. And phones are a target for all kinds of mischief, so it's a good thing. I mean, it's inherently a communicating device. Our phones are getting very sophisticated.

Leo: Well, and they're always online now. So that's...

Steve: Exactly.

Leo: That's the problem with computers these days, too. They're always online.

Steve: On the topic of my being skeptical of new things, when I was running through the mailbag here, I ran across a question from a listener that was exactly something I was going to mention. He says, "I love the security show. I listen to every episode each week at least two or three times. I can't get enough learning about viruses, bugs, spyware, malware, botnets, backdoors, trojans, spoofing, super worms, rootkits, exploits, ghost nets, hackers, et cetera."

Leo: Yay.

Steve: I'm not sure that he left out anything for the "et cetera" to encompass. And he said, "In addition, I love studying cryptography, steganography, biometrics, and computer forensics."

Leo: Steganography is where you put the crypto...

Steve: You hide something.

Leo: ...in a picture or something; right?

Steve: Yes, exactly. I bet, for example, the least significant bits of a high-resolution photo can actually contain, like, a black-and-white image or text or whatever. And he says, "I've been listening to Security Now! over the past year, so now I'm going back in time, starting with the first episode, which has been really exciting."

Leo: Oh, that's nice.

Steve: "I listen to one or more episodes every day on my iPhone while eating, while showering, while driving, and before going to bed. Your show is awesome. Thanks for the hard work, endless security alerts, and motivation to learn more. So my first two questions are, what do you think about Microsoft Security Essentials, a.k.a. "Morro"...

Leo: This was just announced last week.

Steve: Yes. "Have you tested the public beta yet?" And so to answer that question, I have not tested it. It is certainly interesting. I think it's going to be significant. It is

essentially, for those listeners who haven't heard of it, it is what's essentially Windows or Microsoft's next-generation of their Live OneCare, which used to be for purchase. What's significant is this is going to be the first from Microsoft full AV for spyware, malware, viruses, free, which will be available from Microsoft. And it does not only scanning, but on-the-fly interception and detection. It'll be compatible with XP, Vista, and Windows 7, not back to Windows 2000, both 32 and 64-bit versions. You will have to have a genuine certified Windows version that their servers are happy with. So it will not be able to be used with illegitimate pirated versions that don't get the genuine advantage stuff from Microsoft.

At this point it's beta only, and the beta is closed. They had it open for about 75,000 users. It went immediately, bang, and it shut down. So I wouldn't be saying more about it at this point anyway. But certainly it will get a podcast as soon as it's available so that it's relevant to our listeners. And I've got friends where I feel a little guilty telling them that they've got to pay an annual license fee to get AV, or they install a demo version and then it expires, and it tells them, well, you have to pay for this, or it's not going to work anymore. So I think this is going to be significant.

Leo: Yeah, we frequently recommend free antiviruses for that reason. Better a free one, even if it's not as good, than nothing.

Steve: Exactly.

Leo: But you've got to wonder what do Symantec and McAfee do if Microsoft's giving away AV?

Steve: Yeah. This is the steady march of Windows functionality. I mean, once upon a time it didn't have a browser, and it had no firewall, and it had no AV. Then it got a browser, and all the browser people were all in a kerfuffle. Then Windows got a firewall. Oh, no, it's going to put all the firewall guys out of business. Well, you know, initially it wasn't very capable. Initially it was turned off. Now it's turned on. So you argue, well, do we really need a third-party firewall now? And now Windows gets AV. I mean, it was foreseeable. It was inevitable. And I just think, well, the people who were doing those things had a certain window of opportunity to make profit and to get ahead. And I'm sure they'll stay around. They'll come up with enterprise solutions and additional features that Microsoft doesn't have.

Leo: That's what Thurrott said. He said it just gives - they have to branch out. They have to expand.

Steve: Yes, yes.

Leo: But the real question is, first of all, I think we both agree it's great that Microsoft's doing this.

Steve: Yes.

Leo: It's kind of almost incumbent on them to provide a security solution for free.

Steve: Yes. And as someone, as I am, who really prefers lightweight, integrated, nice solutions, I will say that the people who have played with the beta are very impressed with how lightweight it is. Because one of the things, unfortunately, that these third-party kitchen-sink products have evolved into is something heavy, that it's almost more of a problem for your system than actually getting malware. And this is software that you deliberately install. I mean, it's hooked into everything. It's just sitting there really being more of a problem most of the time than the actual problem it's trying to solve.

So the idea that Microsoft has something which is lightweight and simple and free and works and is being updated and - there's some interesting things they're doing that we'll be talking about when we actually cover this in depth in the podcast. But I did want to just sort of do a little shout-out about it and let our users know that we'll certainly be covering it in depth when it becomes relevant.

Leo: Yeah. And of course, yeah, that's the issue, too, is is it going to be as good. If Microsoft gives it away, it's going to be widely used. They're not requiring people to download it.

Steve: No, no. At this point, again, it's like we also weren't, once upon a time, required essentially to use Windows Update. But now...

Leo: Right, now we are.

Steve: ...you're crazy if you don't. And, yes, and things stop working unless you keep yourself current. So again, it's foreseeable that at some point in the future Microsoft will say, well, this is just so good for everyone that it's no longer optional. It's like, okay.

Leo: Not just for everyone, but for the 'Net. I mean, really that's the issue.

Steve: Yes.

Leo: You're protecting not just yourself. And that's the thing I kind of try to beat into people on the radio show. This isn't just for you. This is for the ecology of the Internet as a whole.

Steve: Right, right. In the errata category I have two little blurbs. A reader sent me a fun PDF that was a slideshow that Brian Kernighan of Princeton, in the Princeton Computer Science Department, gave in his CS-152 lecture. And we were talking the other day, one of the questions in our, I think it was our previous Q&A was prompted by a listener's question, trying to nail down exactly what scripting was, you know, what is scripting. And we talked about how it's sort of amorphous. I mean, it's a thing. I mean, I know what it is, and I know what it isn't. But when pressed to really define where the boundary is, it's definitely a fuzzy boundary. Well, what I loved was that in this slide

presentation from Kernighan was a quote from Larry Wall, the creator of Perl.

Leo: The ultimate scripting language.

Steve: Exactly. And so this quote, and I'm not sure where it appeared, where Larry said it. But he said, quote, "Scripting is a lot like obscenity. I can't define it, but I'll know it when I see it."

Leo: Quoting the old Supreme Court, I can't remember which Supreme Court Justice, was it Brennan, who said - I think it was Justice Brennan who said, "I can't define pornography, but I'll know it when I see it."

Steve: I know it when I see it.

Leo: Well, that's actually a good definition. You do know scripting when you see it.

Steve: Yeah.

Leo: And it's hard to make a technical definition.

Steve: Right, right. I love that. And then in my final little bit of bizarre, I mean, an event I could have never predicted, literally, in the last couple Q&As we were talking about the expiration of security certificates. One of the questioners asked, hey, when a certificate expires, what happens? Does it stop working? Can you still use it? Can you still connect to the service and so forth. And I talked about how every so often I'd run across a website whose certificate had expired, and you got this warning notice that said, hey, the certificate's expired. And I talked about how you could imagine behind the scenes they were scurrying around. Actually that's the term I chose. Well, wouldn't you know it, GRC's main security certificate expired, caught me completely unaware, last Thursday. And I was scurrying.

Leo: I got some emails saying does Steve know his certificate has expired? Now, do they not send you a notice saying your certificate...

Steve: They tried. I have no doubt.

Leo: I've done this. I've done this, too, so.

Steve: Yes. They had a three-year-old email address because I signed up for the longest duration certificate I could. And so when I went back and was scurrying, I thought, oh, that's why I got no notifications was that I'm sure that they were trying, and that email address from 2006 was bouncing. And so it's funny because I was all settled in at 5:00 a.m. at Starbucks on Thursday for a nice long coding session. I checked my mail, and

Sue, my bookkeeper, had sent me a note the prior afternoon, late in the afternoon, saying, hey, when I tried to connect to GRC to do our bookkeeping stuff, check in with our ecommerce system, I got this notice about a security certificate expired. And first I'm thinking, wow, I wonder what "she" did.

Leo: It's her fault.

Steve: What is Sue doing wrong now?

Leo: Yeah, I blame Colleen when anything like that happens, yeah. What did Colleen, what did "she" do?

Steve: So I kind of sigh and go to GRC and try to bring up Perfect Passwords, which is one of many things which, I mean, basically all of GRC is wrapped in SSL. You go to ShieldsUP!, you need an SSL connection in order to deobfuscate your connection IP. You use Perfect Passwords to protect the passwords that you're receiving. That's SSL. Of course ecommerce is. And so nothing worked. It's like, oh, my goodness.

Leo: That's not so good.

Steve: So I checked on the page's certificate. And in fact, in Firefox, which of course I'm using now, it said, "Your certificate expired on June 16th." It's like, argh. So I folded up shop and came scurrying home. And a couple hours later we were good to go again. So...

Leo: How much is that? It's pretty expensive, isn't it.

Steve: Oh, it was horrendous. And in fact I'm annoyed with myself because it was $2,580 or $2,850 or something.

Leo: Oh, geez. Oh, man.

Steve: I got it for three years, and I'm buying the best. I use VeriSign, which is the most expensive there is. But for some reason three years ago I had upgraded to their "pro" version, which is not the EVA, not the Enhanced Validation that we've talked about. But I could have spent a thousand dollars, but I would have had to fight with somebody there by phone to downgrade what I bought three years ago.

Leo: Because the pro version's meaningless, really.

Steve: It is. It forces...

Leo: It's an upsell.

Steve: Yes, it's upsell. It prevents you from having a 40-bit key, requiring you to have a 128-bit key.

Leo: But you wouldn't do a 40-bit key anyway.

Steve: Exactly. The export stuff was relaxed a long time ago. Everyone uses 128 bits. I completely could have done it. And then what really bugs me is that, as I think I may have mentioned this once before, last summer when I was working on the DNS spoofability stuff I got a wildcard certificate, *.GRC.com, thinking that I could have used it for anything .dns.GRC.com, only to learn that the star only gives you one domain level of wildcardness. Well, that certificate was still valid for a few more months because it hasn't been a year. And I only bought that one for a year because I was experimenting. So I could have quickly switched to that one, which would have given me then months to resolve the issue of this over-expensive, up-sold, pro certificate. But of course, with the benefit of hindsight, I didn't realize that I had that extra one until I was installing the one I had just bought.

Leo: You were in a hurry. I don't blame you.

Steve: Yes.

Leo: You said, "I've got to fix this."

Steve: Well, yeah, I mean, basically everything that GRC is about was down, and in the most embarrassing way possible. It's like, uh, hello, Steve.

Leo: Oh, boy.

Steve: Yeah. So anyway, it's all fixed, and we're better for three years, and I've got all kinds of bells and whistles. I gave VeriSign a never-to-expire alias for themselves to use, so this time I won't get caught short again. But I did get a kick out of it because I was just talking about what happens when this happens.

Leo: So say that again. So you did something so that you never expire ever again?

Steve: No. What I did was I can set up with my email system various email aliases. And so I gave them their own personal email address for me.

Leo: Ah. So that gets right through...

Steve: Exactly.

Leo: Yeah, yeah, yeah, so you don't miss it again.

Steve: So no one else will ever have it. It identifies where it came from and why. And it'll always map to my current email address.

Leo: Oh, that's clever.

Steve: So they'll always be able to get through to me.

Leo: Very clever.

Steve: And what I did find interesting was that people were still buying SpinRite. They pushed past the scary expired...

Leo: Ooooh.

Steve: No, no, I mean, it's fine because...

Leo: Yeah, but, I mean, there's nothing wrong with them doing that.

Steve: Right.

Leo: But that certificate is what guarantees they're getting a good SpinRite. They should be more cautious.

Steve: No, because it said it expired, that, I mean, it expired right then.

Leo: Oh, okay.

Steve: And that it was from www.GRC.com. So everything was still there except that it had expired some number of hours before.

Leo: Got it.

Steve: So they still had verification that they were at the right site. And they were still secure through the whole purchasing process. They had to make a judgment, okay, how much do I want SpinRite? I trust Steve. This thing just expired. He's scurrying no doubt

somewhere, as indeed I was. So I'm going to go ahead and push through the scary message and purchase SpinRite. So to our listeners I would say use your best judgment. Look at, if you run across an expired certificate, when did it expire? Who did it expire against? If it expired years ago, then I would worry. But if it happened that day, they're scurrying. And if you need a secure connection, you can still get it. And the rest of the certificate is still as good as it was before the calendar changed the pages. It's just that, first of all, this is a revenue stream for companies like VeriSign, which really annoys me, but it does help by forcing this constant reproving who you are. You could argue that the whole issue of these things expiring periodically does increase security, and that's the whole point.

Leo: Right. Are there free certs? Thawte used to do a free cert.

Steve: Thawte did before they got purchased.

Leo: Right. Now they're VeriSign.

Steve: Now they're VeriSign, yup.

Leo: Yeah. Okiley-dokiley. We have some questions for you, Mr. Gibson.

Steve: Oh, yes.

Leo: Would you like to get to those questions?

Steve: Let's do it.

Leo: All right. Michael in St. Louis asks about a review, as you mentioned, of your Kindle DX: I was curious when we're going to get the review you commented on in a previous podcast. I've been really looking at that as a possible reader. But there's no local store I can go to and put my hands on it. That is a disadvantage, isn't it. I'm weary, wary rather, to make such an investment. I read and have a large collection of technical books in PDF format - there's a good reason to do it - and would like to know how native PDF support works on the DX. So you've had it a couple weeks now.

Steve: [Sighing] And I think your original intuition about it was correct, Leo.

Leo: Oh, no. Which was? I forgot.

Steve: A little big and ungainly and difficult to use as a book. I was thinking, okay, fine. I'm an early adopter of technology. I mean, I'm easy about having all these things. This will be my PDF reader. Because the fact is, PDF being a page layout format, as we've

said, you cannot reflow a PDF the way you can reflow a book, which is inherently just a string of text. The PKWARE guys provided me with a big pile of documentation for SecureZIP, the topic of last week's podcast. And so I thought, oh, cool, this will be a great opportunity for me to use the Kindle DX, instead of printing out all these PDFs, as I would have in the past. And they were illegible on it.

Leo: What? Oh, that's very disappointing.

Steve: I mean, I would say unreliably legible. A couple were...

Leo: You mean font size problem? Or...

Steve: Yes, and font color. So it was gray. I couldn't, I mean, if you rotate - the DX has rotation, which unfortunately they're doing the auto rotation thing. And I don't know if they haven't got it down right, or I haven't messed with it enough. But it's the first thing I fumbled around trying to turn off because just in normally holding it, it was switching over into landscape mode when I didn't want it to. So the good news is, you can take over manual control so that you - in the same button where you change the font size is a dialogue that allows you to set what you want for your orientation.

I'm a leftie. And I really like sometimes being able to hold it in my left hand. They removed the page turn buttons from the left-hand margin. It's only now on the right-hand edge of the tablet, which I'm not happy with because now I can't hold it in my left hand and turn the page. It had to have been for reason of cost reduction because additional parts and additional buttons, those all cost something. And so they must have said, oh, well, no one's left-handed, or if they are they can hold it in their right hand. But so that annoys me about it.

If I rotate it into landscape mode, then the virtual PDF page is expanded enough to be legible. But if you have, for example, a two-column PDF, as many PDFs are, then when you get down to the bottom of the first one, you've got to go backwards up to the top. The PDFs don't page align. That is, as you page down, you end up with sort of the bottom of one page and the beginning of the next one coming up, instead of them arranging to align correctly, which is annoying.

Anyway, overall I'm disappointed. I mean, it is truly large. It's funny, too, because after - when I first unboxed it and was looking at it and holding it and oohing and aahing and thinking, oh, look at this magnificent big screen, and you sort of get used to that size, then I said to myself, I wonder what the other one looks like, what my Kindle 2 looks like? And I went right to it and took it out, and it looked dinky by comparison.

Leo: Right, compare it. Because, I mean, this thing is much, much bigger, huh.

Steve: Now, what I will say is that what's compelling about the DX is that the screen as a percentage of the total surface is much larger than on the Kindle 2. The Kindle 2's keyboard is much larger, and the screen seems very small in the overall size of the Kindle 2. Whereas certainly the DX has just a magnificent screen. But I think it's sort of in between. It's not good enough to be used as a general PDF reader. Certainly, I mean, I have read PDFs that are magnificent on it. And if I were, for example, printing an RFC,

a multipage Request For Comment, an RFC document from the Internet, I could print it to a PDF, move the document to my Kindle DX, and read it just magnificently. It'd be perfect. So PDFs you make and PDFs of simple text, they work beautifully. But that's not always what your source material is.

And I found many of the PDFs from the PKWARE guys, for no fault of them - for example, I did end up reading them on a regular PC browser, and they were fine there. But the DX did not do them justice. And so I would argue that for $500 people are going to be disappointed if they really think they're going to be able to read any PDF they encounter. It's really the case still that a higher resolution color screen like you have on any laptop or tablet is a better solution for PDF. Or printing it out on paper.

Leo: Oh, well.

Steve: So again, I think your intuition was right. I could wish for a Kindle 3 which would be the physical size of the Kindle 2, but much more of it as screen. That is, do what they did with the DX and squeeze the keyboard down. Because you hardly use the keyboard...

Leo: Yeah. You use it to order, and that's it, pretty much.

Steve: Yes, exactly. And so squeeze it down, give us more screen, but keep it paperback book size because, I mean, that really - you were right, Leo. The convenience of it being that size, compared to it being of the size of the DX. It's just big. The problem is, there's no way you're going to be able to read page documents on a small screen. It's just - they're going to be too small. So it's just like the problem with the keyboard. You can't have a small keyboard and full touch-typing speed because you can't. You have to have a full keyboard in order to run at the speed that you normally do. So that human factors interaction is just - it's a fact of life.

Leo: Yeah. Oh, well. I'm glad you spent the money, not me.

Steve: Yeah.

Leo: Thank you. We all owe you a debt of gratitude. I'm happy with the Kindle 2. And I took it with me to the beach. We were spending the week at the beach house - at a beach house we rented. When I say "the beach house," it sounds like I own one. I do not. We rented a beach house. And it's been great on the beach, sitting on the beach. The sun is shining, and it's really legible. Which a laptop would not be.

Steve: No, that's very true. And I have to say also, while I'm dunning on the DX, it's also heavy. The people I gave it to said, oh, I mean, it's like - so you try to hold a corner, and it's trying to twist itself out of your hand because it's heavy enough. I think what that says is that there's a lot of battery in there. I think there's probably a very large surface area battery...

Leo: Lot of mass.

Steve: ...because it does turn pages more quickly than the 2. I think they're running the processor faster, which they can afford to do - which is going to consume more power, but they can afford it because they've got much more battery area spread out in this DX than they do in the Kindle 2. It's probably about twice the area. So, I mean, it's snappy performance. I like that about it. But it's just - it is unwieldy. It's too big.

Leo: Well, thank you for that, and I'm glad I waited.

Steve: Yeah.

Leo: For you. Another question. This is from Steve Whaley in Lexington, Illinois. He asks: Hey, you talked about SecureZIP, and you said it was free. Really? I'm unable to find a download of this product that's free. It seems PKWARE wants $39.95 per user for home PCs. Am I missing something?

Steve: Many people wrote variations of this question. So I apologize to our listeners for not having given you the simple URL. I'm sure I said just put "SecureZIP" into Google, and it'll take you right there. It does, but the URL is SecureZIP, so I should have just said that: www.securezip.com redirects you to a page...

Leo: Oh, yeah, that says right there "Free Download."

Steve: And it is. And it does have that 30-day feature expiration that I mentioned where it'll give you the Office integration, the Office and Outlook email integration for 30 days. And then that dies, yet everything else about it stays fully functional. And if you don't want to be able to, like, if you don't need to send a piece of email literally with a single click, or save a Word document with a single embedded function, then that free post-30-day SecureZIP, which continues to function just fine, is really all you need.

Leo: Another question from a professional programmer in Sacramento. I love that. His name is Damien Eversmann. He wonders why coding error equals remote code execution: Steve, first, ditto to what everyone always says. I've been listening since Episode 1. Hope you and Leo keep it up for some time to come. So here's my question. I'm a professional programmer. I've been doing it for about 15 years now. I understand most of the programming errors you describe when you talk about various software flaws that vendors are patching in your weekly security updates. But what I don't understand is why it always seems that every coding error means remote code execution vulnerabilities.

In my experience, my coding errors just mean my application ceases to work. It freezes or crashes or quits. But every error you mention every week seems to mean remote vulnerabilities. Buffer overrun equals remote code execution. String index mismatch equals remote code execution. Array index out of bounds equals remote

code execution. It almost seems like programmers would need to try to make remote code execution so available. Sometimes after your reports I feel like remote code execution flaws seem more reliable than a program functioning as described. What am I missing? Again, love the podcast. Looking forward to Mac-SpinRite so I can run it without removing drives from my Macs. With a PR person like Leo, I think you'd sell a few thousand copies in the first five minutes if it were available. Thanks so much, Damien. I'd like to echo that, by the way.

Steve: What Damien is missing is that the show talks about remote code execution because it's a bad thing.

Leo: Right.

Steve: So the bugs which software has and which are not bad security vulnerabilities, we don't talk about.

Leo: They just crash.

Steve: There's plenty of other bugs in software that just makes them crash. Where they're bad, they crash, people are annoyed, but there happens, exactly as he is suggesting, there happens to be no way of preloading the content of the buffer which you overflow into, or leaving stuff on the stack which you end up executing. We understand how it is that some of the mistakes result in remotely provided code getting executed. We've talked about those earlier in the beginning podcasts of this four-year run that we have so far. So our listeners understand that. It is the case that, exactly as Damien suggests, many bugs don't provide you with the means of loading code at the same time. But those aren't problems of security. So we don't talk about those.

So there are definitely plenty of problems that do not create this kind of remote code execution. There are also problems that just, you know, they end up with like a privilege escalation where you're able to - code that is running is able to elevate its privileges from your limited user status to admin or something. And so there are other tricks that can happen. The worst, of course, is that without you knowing it, you visit a website, and now you've got something running on your machine as a consequence of viewing that page. Those are the exciting problems. Those are the problems that make the news and that force Microsoft to jump through hoops and get things patched, or Adobe, or Apple, or anybody who's now in this Internet-connected world. So the point is, yes, it seems that all these problems cause remote code execution because those are the ones we talk about.

Leo: We only talk about those.

Steve: Those are the security problems.

Leo: Although, credit where credit's due, these hackers work really, really hard and

are quite ingenious in finding code, finding ways to inject their code into these overflows. I mean, it's nontrivial to do that. It's not...

Steve: Yes. I've mentioned, for example, the guys at eEye, who have a whole lab full of machines. And these machines are literally throwing random API calls with random parameters and packets with random data at the operating system and waiting for it to crash. When it crashes, then they go in forensically and find out what packet it was that caused the crash. Then they go in and disassemble the processing of that packet to look at why it crashed.

So, A, they've got a crash. Okay, that's news because it shouldn't crash. But then, by looking at every detail of the nuance of what preceded the crash, they look to see whether, for example, the crash occurred when the computer executed just some random garbage that was in the packet. If so, then they think, wait a minute, let's give it a packet which qualifies for the crashing, that is, that makes it crash. But if possible, can we put other data in that packet that would also cause it to execute the data we choose?

So they literally, they reverse-engineer the exploit from a seemingly random occurrence. Most of us, the machine crashes, and we curse its maker and reboot, and we're going again. But security researchers take that event of a collapse and say, ooh, could this have been much worse than just a random-seeming event? And so, yes, you're right, it takes, you know, it's serious kung fu to back this out into an exploit. But some people have nothing better to do. Some people get paid for it. Some people sell their exploits on the black market, unfortunately.

Leo: Because there is such a lot of money to be made, there is some incentive to do this extremely difficult and time-consuming work.

Steve: And Leo, if you had said to me this was what we'd be talking about 20 years ago, I'd have said, this is science fiction. I mean, it makes a great...

Leo: Yeah. It doesn't seem possible.

Steve: ...makes a great story. But come on, it's not - it's like I mentioned Neo selling the little disk in the opening scene of "The Matrix." It's like, come on.

Leo: Couldn't happen.

Steve: In the future we're going to have fixed all this; aren't we? Well, apparently not because the future is here.

Leo: I think it's going to be worse as we get older and there's more code.

Steve: There's no indication that it's getting better, Leo.

Leo: Yeah. And, well, and I bet you there's some questions in here - we talked a little bit about the idea of using languages that prevent this kind of stuff on previous episodes. And as you pointed out, as long as there's programmers, there'll always be some mistakes.

Steve: And those aren't fun.

Leo: They're no fun to work with.

Steve: Those languages. We want bare metal, written for the geeks [indiscernible] language.

Leo: Let's get in there, yeah. Joseph Vollmer in Waterloo, Ontario, Canada wonders whether WPA/WPA2 is "quickly crackable." I'm fully up to date with all the episodes. Started listening to Security Now! in January 2007, and I've been listening ever since and love the show.

I'm an IT support pro, and a bunch of my co-workers claim they can, or it is possible to, crack WPA and WPA2 without much trouble at all. Yeah, the usual swagger. I always argue, saying if you set it up properly, like using AES and use one of Steve's pseudorandom 63-character printable ASCII characters, it's not going to be crackable in a usable amount of time. They claim there are all kinds of readily available hacking tools that allow you to crack it quickly. They say because of the number-crunching power of GPUs it can be cracked quickly using hacking tools. I agree cracking WEP, as we know, is easy. Do that in 30 seconds now. Could you please shed some light on WPA? I'd appreciate it. I continue to argue with them, saying it's not possible. Which I always say you've got to set it up right, of course. If you use dog1234 for a passphrase, no problem.

By the way, I'm a proud owner of SpinRite. It's saved my bacon many times. Now if only work will finally listen to me and buy a site license, all will be well. I'm working on that One day I hope I'll get it approved by management. And I will not stop until it happens. So, Steve, yes or no? WPA2, easily crackable?

Steve: Joseph is absolutely right.

Leo: I thought so.

Steve: And I just - I liked the question because it sort of feels like sort of this is coming from youngsters, you know, young...

Leo: I could crack it. Eh, no problem.

Steve: ...wannabe hackers, yeah, exactly. Joseph should just say fine, show me.

Leo: Crack it.

Steve: If these tools are available, if they're easy to do, put your evidence on the line. Show me. I mean, he could make as large a bet as he wants to. If he uses one of GRC's random passwords, I mean, I use those myself. The other day I needed a random string for the header of a file to be used as an index mark for some versioning stuff in the DNS benchmark. I went to my own site, to my page. Fortunately the security certificate was still valid at that point. And I had it generate those numbers for me, and I grabbed them, and I used them because they're as random as anything you can get. So, I mean, Joseph could make - he could make a bet as large as he wanted to, saying okay, great, crack it. And it's absolutely safe. I mean, this is - there is this sort of, as you said, swagger is a perfect term for it, among young hackers who read stories and hang out on BBSes. And they're these people who to really lay people sound like they know what they're talking about. But they're just full of it.

Leo: Yeah, they throw in the little tech obfuscation, oh, you use the GPO.

Steve: Yup, just put some jargon in there, and it's like, oh, that sounds convincing. Well, it's just not the case. There is, exactly as Joseph says, there is no known problem at this point. And it was highly vetted, unlike WEP. The WPA protocol has really been well designed and well thought out, and we know of no way to get around it. And it's been designed also so that, for example, even GPUs are able to crank through, we're talking about many bits. And as you add a bit, every bit you add, as we've said, doubles the length of time that is required even from a brute-force attack. So you could use a room of graphic processing units designing this, and they're still going to be churning away for a long, long time. Joseph would get his money from his bet.

Leo: Let's see. A Security Now! listener in California has asked to be anonymous while asking about a homegrown VPN client: As a consultant I'm often asked to use a client's VPN for remote access to their network. My current client has a homegrown VPN client. It is an ActiveX add-on to IE. Is there some way I can determine what this VPN client is doing? Is there, I don't know, a keystroke logger I could use? Is it capturing non-VPN activities? Can it provide information about what I do for other accounts on the same computer? Can it be used as a gateway to install rootkits or other technologies on my system? Please sign me Anonymous in California.

I see his concern. He's being asked to run software, strange software on his system, and he's got other clients to protect. He's not sure it's safe.

Steve: Yeah, it's a great question. And, I mean, you can see the position he's in. They're saying, oh, well, this is our homegrown VPN client. Well, first of all, I'm skeptical of some random company home-growing their own VPN client. It's probably something that they got from somewhere else. Who knows...

Leo: As you know, because you've tried to - you've been writing VPN software, it's nontrivial.

Steve: Yes, exactly. It's a nontrivial task. So I'm wondering where it really came from. But even so, this is a great question because, I mean, we could broaden it a little bit and say, okay, I'm somebody who, exactly as you say, Leo, I'm responsible for the security of many different people, many different clients. One client, for example, wants me to install something random on my machine. Well, how do I make that safe? How do I know what it's doing? How do I know that it's aboveboard? And this, I would say, is a perfect example of where wrapping this thing in a virtual machine makes sense. If I were in this situation, I would be running one of the VMs, like VMware. And, I mean, especially, hopefully our listener is using Firefox normally. This thing is an IE ActiveX add-in. So put it in a virtual machine. Get Windows running there.

Leo: That's a good idea. That's a very good way to do it, yeah.

Steve: Yeah. And then it's going to have some isolation. Then you know when you're not running it, you're not running it. It's going to have full networking abilities. It's going to be able to still do its VPNness. And you can full-screen that VM so that you can even forget that you're in a VM. But when you shut it down, you've shut it down. And it's very unlikely that it's going to be able to get out of that because the VM as we've looked at provides high levels of integrity. It's not necessarily absolutely bulletproof and perfect. But something that's not written to bust out of a VPN, I mean, out of a virtual machine, is just not going to be able to. It's not going to stumble out of it by mistake. So I think that's the best you can do. I mean, the alternative is dual boot. Set up a separate boot for stuff, like for this guy, or use a different machine. But it certainly is worth noting that this is a concern. I think that's a great concern.

Leo: Steve, another question for you from our great listeners. This is Anthony Fitch from Blaine, Kentucky. He says he saw it happen firsthand: First of all, I've listened to every episode of Security Now!, and it has filled in all the gaps in content that were missing in my formal classes in college. That's awesome. This show has lead me to win First Place in the Computer Concepts category in the Phi Beta Lambda state competition two years running. Steve, that must make you feel good. That's awesome. That's fantastic.

Steve: That's very cool.

Leo: The reason I'm writing is to share with you that you were right about the insecurity of Eastern European ATMs. On a recent - two weeks ago - trip to Europe, while in the Czech Republic, one of the members of our tour group had her debit card number stolen because she used an ATM in that area. This is good for me to remember because I'm going to China next week. Her bank kindly returned the money that had been stolen because they emptied her bank account, although it was an extreme headache due to time zone differences and of course the costs of making phone calls back to the states.

Thank you very much for your time. And as much as I would like to, I do not have a SpinRite testimonial yet. That's good. As long as you have SpinRite, you probably don't need to do a testimonial. Everything just works. P.S.: I'd be honored if you'd read this on the show. Of course, Anthony. And that's great.

Steve: I thought that was just a nice little tidbit from a listener, that we've talked a lot about the inappropriate use of Windows in mission-critical environments. And also we did cover the security news of trojans being found in a whole bunch of Eastern European ATMs. And a listener of ours knew somebody who - he was standing there when it happened. So it's like, yep, this stuff is real.

Leo: Yup. And it does remind me, as I head off to Asia - I'll be in China, Korea, and Japan. And, I mean, but that's what you do when you travel nowadays. You don't carry traveler's checks anymore. A lot of people don't even take them anymore.

Steve: Right.

Leo: You use the ATMs to get the local currency.

Steve: Yeah. I would say what you could do, if you can, don't use a card that's associated with all the cash that you have.

Leo: That's a good point.

Steve: Set up an account that you can afford to have...

Leo: Yeah, I do, I have - oh, that's a good idea. Okay, I'll bring my - I have an ATM card that I don't use very - it's like a secondary account. Great thinking.

Steve: Yes.

Leo: And I think, if I make sure to use it inside of banks, I'm probably a lot safer than if I just use one on the street.

Steve: Yeah, but again, belt and suspenders. I would also just use an account without a ton of money in it.

Leo: That's a very good idea. Thank you. Rick Huebner in Melbourne Beach, Florida is worried about "same plaintext and multiple ciphertext in SecureZIP." I'm sure he'll explain what that means.

Steve: Get your propellerhead on.

Leo: Here we go.

Steve: Get your hats.

Leo: Here we go. Steve, in the discussion on SecureZIP you said, and I quote, "So the idea is, if you want three different people to be able to decrypt this ZIP file, you're able to attach their certificates to that file. And essentially it takes their public key and encrypts this one-time-use symmetric key for each of them and connects it. So that when any of them receive it, they're able to open the file, and they're able to inspect the certificates that are bundled along with it."

Steve: Yup.

Leo: Now, here's his question: Does the fact that one recipient now knows the plaintext symmetric key, has the ciphertext for the other recipients, and presumably can get the other recipients' public keys because those are stored easily, widely, would it make it easier to crack the private keys?

I thought in one of your previous episodes you said you never want to encrypt the same message with different keys. Or was it that you never want to use the same key to encrypt two messages? Either way, does this in some way weaken the cipher? If so, is it something ridiculous like going from 100 billion years to 10 billion years?

I've been a listener since Security Now! 001 and actively read the newsgroups, as well as owning a copy of SpinRite that saved my father-in-law's bacon. Man, SpinRite on a newly purchased 1.5TB drive takes a lot of time. Also I SpinRite my two Series 2 TiVos and my old dinosaur Series 1 TiVo, all with additional hard drive capacity, because my wife would kill me if she lost any shows. That's actually a very good idea. Those drives get thrashed on a TiVo.

Keep up the good work. I can't wait for CryptoLink to come out to replace my current Hamachi implementation. Any chance it will support Windows Mobile devices?

Steve: Okay. So great question from Rick. What he's saying is, and he's exactly right, is that in the case where multiple certificates are attached to - in this case he's talking about the SecureZIP system where, for example, you zip and you want to encrypt the content so that three different people, each with their own certificate, are able to decrypt it; but no fourth party, for example, nobody else can. The way that's done is that a 128 or 256 or 192, however many, however long the key is, a cryptographic-quality, high-quality random number is chosen out of the air, called a "nonce" in crypto terms. It's something that's just random, and you're just going to use it once. That is used as the symmetric key for performing the bulk encryption of the content instead of using, as we've talked about, you don't use - you don't do the bulk encryption with the public/private, the asymmetric key because it's very time-consuming and number-crunching intensive. Instead you just choose a random key to do your bulk encryption, and it's that random key that you then encrypt using the asymmetric, the so-called public key technology.

So this random key is encrypted three times, once with each certificate. Not serially because that would require that all three be used to decrypt it. You would do it like in reverse order then. But instead I mean that, like, that random token is encrypted once with one certificate, so now it's there. It's encrypted again with the second certificate, and a third time with the third certificate. So now you've got three encrypted versions of the key. Each one can only be decrypted with the matching private key for that

certificate, which isn't available - it's only available on the systems where those certificates are installed for these three different people. So now the zip file goes off to them all.

So Rick's wondering if one of the recipients gains an advantage of any sort in this scenario. Because he's got one of the certificates with a private key, he's able to decrypt the encrypted nonce, that encrypted symmetric key which is intended for him. That allows him to get the plaintext version of the symmetric key, which is what he needs in order to view the contents of the zip. But he also has the two other encrypted versions of the key which were bundled into the zip file. And he's got the public keys which are publicly available for the other two people. So he's saying, hey, now I've got a lot of information here. I've got both the plaintext, which I decrypted using my certificate, and the ciphertext which is individual for each of the certificates that were created, and the public key. Do I have an advantage?

The answer is absolutely not. The good news is, this is exactly what the public key, the asymmetric key technology was designed for. A perfect example is the normal case of digital signatures. Remember that when you're doing a digital signature you take a document, and you hash it using a cryptographically strong hashing algorithm. Now the signer will take their private key and encrypt that hash and then include it with the document. Now the recipient gets the document and wants to verify it. How do they do that? They decrypt that signed hash with the signer's public key, turning it back into the plaintext version of the hash. Then they independently hash the document using the same hashing algorithm and compare their resulting hash to the decrypted hash. So the information they have is exactly the same as the information that one of the zip file recipients would have. That is to say, they have both the plaintext and the ciphertext of - oh, and the public key, the same information. And as we know, the public key technology is secure against this sort of scenario. So the SecureZIP system, where you've got multiple recipients, is no less secure because of the way it implements the public key technology. But great question.

Leo: Yeah, yeah. And actually when he stated it I thought, oh, yeah, that makes sense. So I'm glad you clarified.

Steve, we're out of time for this episode, but not out of questions. Every other episode we answer your questions. You can submit them right now to GRC.com/feedback, and we will get to as many questions as we can, each and every even number, mod 2 episode. Meanwhile, don't forget to go to GRC.com, that's Steve's website. It's short for Gibson Research Corporation, now with a shiny new certificate for your security [laughter].

Steve: Good for three years at least. We don't know what'll happen after that.

Leo: And when you're there you can try ShieldsUP!, his great program to test your router. You can download all sorts of free, wonderful programs. And of course get SpinRite, the world's finest hard drive maintenance and recovery utility. We also, or Steve also puts a transcript of every show up there so you can read along, or cut and paste into your questions if you should choose next time. You can also listen to the 16KB version or distribute that for the bandwidth-impaired. It's all at GRC.com. Steve, we will see you next time on Security Now!.

Steve: Talk to you then, Leo, thanks.