SECURITY NOW!

Transcript of Episode #215

Security Maxims

Description: Steve and Leo discuss the first portion of a collection of pithy and apropos "Security Maxims" that were assembled by a member of the Argonne Vulnerability Assessment Team at the Nuclear Engineering Division of the Argonne National Laboratory, U.S. Department of Energy.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-215.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-215-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

Leo Laporte: Bandwidth for Security Now! is provided by AOL Music and Spinner.com, where you can get free MP3s, exclusive interviews, and more.

This is Security Now! with Steve Gibson, Episode 215 for September 24, 2009: Security Maxims. 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!, everybody's favorite show about protecting yourself online. And here he is, the guru of security, the man of the hour, Mr. Steve Gibson of GRC.com. Hey, Steve.

Steve Gibson: Hey, Leo. It's great to be back with you again, as always.

Leo: Nice to have you.

Steve: Yeah, we've got a really - some fun content this week. I mean, we always have various flavors of fun. This is something we've never done before. A couple months ago I ran across - and frankly I can't remember whether I stumbled on it, or a listener might have said, hey, check this out. So if I got it from someone, I apologize for not acknowledging them. But it was a page of what this author called his "security maxims." I looked up "maxim" in the dictionary to get the exact definition, and it's defined as "a succinct formulation of a fundamental principle, general truth, or rule of conduct." And this guy is Roger Johnston, who's got his Ph.D. and also his CPP credential, which is Certificate of Protection Professional.

Leo: Oh, I never heard of that. That's cool.

Steve: He's with the Argonne Vulnerability Assessment Team, the Nuclear Engineering Division of the Argonne National Laboratory, which is a division of the U.S. Department of Energy. So these are...

Leo: You know, that's interesting. Because the Department of Energy was the one who created CERT, the Computer Emergency Response Team. I mean, they have been, until recently, they've really been carrying the torch for security in the government, the national government.

Steve: Right. Well, you know, someone's got to do it.

Leo: Yeah. And I guess if they have nukes, they probably - it's as good them as anybody.

Steve: And so a couple months ago I wrote to Roger. And I said, hey, you know, I kind of wanted to get a little background. I thought this would be a really fun thing for you and, well, for us to discuss just sort of interactively, to go through these really fun sort of succinct, pithy maxims in the context of everything that we've been discussing for the last couple years. So I said, hey, I wanted to get a little more background, where did these come from and so forth.

And he wrote back, he said, "Steve. The most recent list of maxims is attached." And so he sent those in his response. And he said, "Most of the maxims are my creations over the last several years or so. Being a vulnerability assessor for physical security makes one pretty cynical. Or maybe you need to be cynical to see security problems. Or maybe both are true. Anyway, these maxims were developed partially out of frustration at seeing the same kinds of problems over and over again. They're offered partially tongue-in-cheek, but partially not, since they are more or less true." And actually I think they're very true. I think they're just wonderful.

And he said, "Oddly, cybersecurity people get more excited about these maxims than physical security people, although they were really developed more with physical security in mind. Over the last couple of years security professionals who liked the maxims would offer some of their own. If I liked their suggestions, I tacked them onto the list." So we're going to today discuss - and we've got so many, we won't get them all into this podcast. But that's fine because it's just sort of something fun we'll bring out from time to time and dust off and continue going through the list.

Leo: How many are there?

Steve: There's a ton.

Leo: There's six pages I'm looking at right here.

Steve: No, no. You just have the first chunk. I've got more...

Leo: Oh, there's more.

Steve: Oh, yeah. Because I thought, okay, we're never going to get through this many. So we'll do as many as we can in a reasonable amount of time. And then at some point in the future I'll say, hey, we're going to do Security Maxims Part 2. Because I think people are going to get a big kick out of them.

Leo: This is good. So we aren't just going to give you the maxim. I know Steve. You're going to tell us what it means, how to implement it...

Steve: Oh, exactly. I wanted to break them down...

Leo: ...what the implications, yeah, I think that's great.

Steve: ...give examples, discuss each one, exactly.

Leo: Love that idea. Well, before we get there, we have to mention our sponsor. And I know you probably have security news and errata to cover, as well. So let's...

Steve: We do. And I've got some bad news about what happens when you try to spy on your girlfriend.

Leo: I don't know if that's bad news or good news. I guess it depends if you're the boyfriend or the girlfriend.

Steve: Well, if you're the hospital where she works, it's bad news.

Leo: Oh, boy. All right, Steverino. Any news? Any security news you want to talk...

Steve: Well, we do have some news. I think I've mentioned - I know I've mentioned a couple times over the last few weeks some people have written in saying, hey, Steve, we think you're being a little unfairly rough on Microsoft. And it's like, okay, maybe. I'll keep that in mind. But I did run across Apple's news about their September 10th update, their security update 2009...

Leo: 2009...

Steve: ...dash 005. And Apple is notoriously close-mouthed about what's going on. In fact, their formal statement on their update site is, "For the protection of our customers, Apple does not disclose, discuss, or confirm security issues until a full investigation has occurred and any necessary patches or releases are available. To learn more about Apple's product security, see Apple product security website." So that sort of has the effect of obscuring a little bit about what's going on because when the details come out afterwards, it's afterwards. So it's no longer newsy. But what struck me was that I really think we're very rapidly approaching, if we're not already at, the point of being able to say that the Mac is no more secure than Windows. That is, than Windows-based machines.

For example - and this is just a brief summary. I thought, well, I could go over the details, but it would just be going on forever. So in summary of what Apple slid into the Mac OS without giving any details a couple weeks ago, there was a buffer overflow error in their handling of alias files that could have resulted in remote code execution. There's a memory corruption error in Resource Manager in its handling of resource forks that could have resulted in either application termination or remote code execution. Multiple vulnerabilities identified in the ClamAV which was distributed only with the Mac OS X Server systems, but several of those vulnerabilities could lead to remote code execution. An integer overflow error in the handling of images with an embedded ColorSync profile. And actually we've seen those before in Mac OS security updates.

An integer overflow error in core graphics, the way it processes PDF files, that could result, if you opened a PDF, in remote code execution. A heap overflow error in the core graphics caused by drawing long text strings. A null pointer dereference error in CUPS, which is the Common Unix Printing System that the Mac uses. A heap overflow error in the USB back end for CUPS. Multiple vulnerabilities in Adobe's Flash Player plug-in, which, okay, is not Mac's fault, but it was there. And some of those could have led to remote code execution.

Multiple memory corruption errors in Image I/O subsystem in the way it handles Pixar film-encoded TIFF images. A design issue in the Launch Services system which can cause an unsafe file to be opened automatically. A design issue in Launch Services, as a result of which there's no warning while attempting to open a downloaded content which is unsafe. An implementation issue in MySQL that might lead to an escalation of privilege. Multiple vulnerabilities have been identified in their PHP - again, not Apple's fault, but a component that they were including with, you know, open source that can result in remote code execution. An error in Samba as it fails to perform adequate checks, thereby leading to unexpected sharing of folders. And finally, a cross-site scripting error in their wiki server in the way it handles requests that have non-UTF-8 encoding.

So this sort of all got fixed, which is good. But, I mean, given what we've been seeing over the last year, I would say that - and in fact our security maxims are going to be substantiating this because we'll recognize sort of the standard common wisdom of that - I would say that the Mac is pretty much at a par with Windows. That is, that as a consequence of the reality of the difficulty of security, how complex modern operating systems are, whether from Microsoft or Apple or the open source community, mistakes get made. And bad guys, the more they look, the more mistakes they find. And we're really seeing an increase in the rate at which problems are being found in the Mac. Not, I think, because there are more problems than there were, but because we're looking more closely. You know, there are more Macs, and more people are using them. The bad guys have them. And as we said before, malicious people can't find mistakes in systems they don't have. They find them in the machines that they're able to inspect closely. So...

Leo: One thing I'd point out is more than half of the ones you talked about, CUPS and Samba and ClamAV and PHP and many, many more of those you talked about are open source projects.

Steve: Right.

Leo: Because Darwin is open source, and much of the software that runs on Macs are open source. So you're going to - the same exact thing you just said can be said about Linux and open source operating systems. In fact, it could be said about every operating system.

Steve: Correct. And that's my point is that...

Leo: Well, and the reason I bring it up is that for a long time Windows advocates have pointed to Linux and said, look at all the patches in Linux software. And I think that that's kind of an unfair critique. If software is being patched, and openly being patched because of problems being found, that doesn't mean that - all software is bad, but it doesn't mean that this software is worse than other software. In fact, it means it's being patched more quickly. You could make the counter case that a closed-source system like Macintosh or more likely Windows, they may know about many, many more vulnerabilities that aren't being patched. So your vulnerability count could be lower. It does not mean you're safer. Could mean quite the contrary.

Steve: Yeah, and in fact I would argue that it's probably impossible to make a meaningful comparison, to answer...

Leo: Exactly. Exactly.

Steve: I mean, people, all of the fan boys in any camp want to say theirs is worse than ours, ours is better than theirs. But I don't know that you can make, I mean, the problem is, this is not black and white. All of this is grey.

Leo: Yeah, I'm just saying that counting vulnerabilities, as you're just saying, is kind of meaningless. It doesn't say anything one way or another.

Steve: Right. I completely agree.

Leo: I guess what you could derive from it is what you did derive from it, which is people are looking more closely and finding more. But we don't know. It could also be Apple's revealing more, and it never did before; or Apple never patched stuff before, and there was this stuff. That's my sense. In fact, Apple's been criticized for a long time by open source advocates for having a lot of older open source software on their system that has known vulnerabilities and not responding to that.

Steve: Right. But I guess certainly what we do know empirically is there seems to be a much more continual flow of updates now.

Leo: Thank goodness.

Steve: Yes.

Leo: That's the way it ought to be; right?

Steve: Exactly. Yup, these things are getting fixed as they're being found.

Leo: I think a lot of users, like to my radio show, get concerned when they see all these patches. It implies there's something bad going on. Oh, my gosh, that software is horrible. And it doesn't necessarily mean that.

Steve: No. I would say all it means is that people are looking more closely and finding things that need fixing. Which is the case in any system, exactly as you said. Speaking of which, I had an interesting little statistical tidbit. Remember we talked either last week or the week before about how the new versions of Firefox were going to be automatically notifying their users if the Flash, if the Adobe/Macromedia Flash plug-in was out of date. In the first week of doing so, 10 million Firefox users clicked through and updated their version of Flash.

Leo: It's kind of mind-boggling, the numbers; isn't it?

Steve: 10 million. Apparently the normal click-through is something like three or four percent. And this time it was 30-some percent. I mean, it was a huge success. It turns out that apparently 75 percent of Firefox users were running outdated versions of Flash.

Leo: Wow.

Steve: And so Mozilla considers this campaign...

Leo: Victory, yes.

Steve: ...to be a tremendous success. And they are planning to partner with the providers of other popular plug-ins to do the same, basically to mature Mozilla so that it will be continually aware of updates, sort of on behalf of plug-in manufacturers, and let people know that there's a new version available. So I thought it was really interesting that there was, I mean, this was a huge win really for everyone.

And it sort of does sort of represent what we're seeing in terms of the operating system and web-based ecosystem where the browser is becoming the platform. The browser is where you run applications. It's where you - the way you interact with the Internet is more and more through the browser, rather than through lots of independent standalone apps. So here's the browser needing, sort of much like an operating system, to become responsible for the security of the user's experience, which means indirectly the browser that is containing these plug-ins is having to become - is fortunately taking more and more responsibility for the safety overall of the content that it delivers.

Leo: Constant debate, who's responsible; right?

Steve: Yes. Everyone wants to point fingers. I'm really impressed that Firefox said, okay, we're going to step up and let people know if they've got old versions of Flash.

Leo: And you wonder, how does Adobe feel about this? Good or bad?

Steve: I would think just...

Leo: They ought to feel good; right?

Steve: Yes, yes.

Leo: But in some ways it's an indictment of them for not doing it themselves.

Steve: Well, it's funny because I noticed that on some of my machines I've got an InstallShield Update Manager. And I'm Mr. Minimalist. I want as little stuff running around in my machine as possible. And so I'm a little annoyed that there's an InstallShield Update Manager. But it does tend to aggregate the updates of several different disparate products which have used InstallShield to install themselves. And it's like, okay, well, I guess that's better maybe than each one of them independently needing to be running something all the time to check and see.

I think the best model from my standpoint is when you run something, to have it at that time, if you've configured it to do so, check to see if there's a newer version of itself. And also, of course, check to see when the last time was that it looked, so it's not always looking. And many programs now say, yes, check for updates, and no more often than once a week, or once a month, or you're able to configure that. Which I think that's a nice compromise. But clearly this new model of we're connected, and software is able to check in with itself, is where we're headed. And in fact I've implemented exactly that facility now with my stuff. We'll see that for the first time in this ever-forthcoming DNS benchmark.

Leo: Okay [laughing]. Stop teasing us.

Steve: I just got thrown a curveball. Somebody was commenting that they wanted to get all-green status, but their servers were rearranging themselves from one run of the benchmark to the next. So now I've just finished adding an awareness of statistical significance to the difference in timings so that the benchmark will - it takes the standard deviation of all the samples and does a statistical significance calculation to determine if, okay, yes, the average of these samples was a little faster than the average of those. But based on the spread of samples that we obtained, we can't say with greater than 95 percent certainty that it's a statistically significant difference. So it does all that now, too. So I'll get finished with it one of these days, and we'll do a podcast on it.

Leo: No hurry.

Steve: Meanwhile...

Leo: Take your time.

Steve: Meanwhile, Robert McMillan, reporting for Computerworld, carried an interesting story that caught my attention. A 35-year-old man in Avon Lake, Ohio named Scott Graham has his tail between his legs at the moment, and in fact he's set to plead guilty to federal network spying charges. He purchased for $115 a program called SpyAgent, which he sent to his ex-girlfriend's Yahoo! email account.

Leo: Creepazoid.

Steve: Yes. He wanted to spy on his ex-girlfriend.

Leo: Jerk.

Steve: Unfortunately, she works in the local hospital's pediatric cardiac surgery department. And as a consequence you could also argue of the hospital's lack of sufficient security, she used her web browser, went to Yahoo! email, opened her email and installed SpyAgent into the machine at the hospital's pediatric cardiac surgery department, creating among other things a regulatory nightmare for the hospital because then, over the course of about two weeks, the spyware on her machine emailed to Scott Graham, the creepy ex-boyfriend, more than a thousand screen captures of what was going on on this sensitive machine, including details of medical procedures, diagnostic notes, and other confidential information relating to 62 different hospital patients. He also obtained email and financial records for four other hospital employees. So he's now facing $33,000 in damages from the hospital and a maximum sentence of five years in prison. So anyway, I...

Leo: Good.

Steve: Well, yeah.

Leo: Geez.

Steve: Yeah. And, I mean...

Leo: So that's - that's illegal to do that. Even though people sell this product, it's illegal to...

Steve: And it's amazing to me that people can sell this product. They say, oh, it's for parents to keep an eye on their children and the way they're using the computer. And it's like, okay...

Leo: But they know perfectly well that's not the only people who use it.

Steve: Yes. I mean, I would venture to guess that 99 percent of the purchases and use of this kind of a creepy tool is for this kind of application. And of course this is - so his intention was that she would run this from her machine at home, infect her machine at home, and then he'd be able to figure out if she was dating somebody else or who knows what this creep's plans were.

Leo: I hope they slap the wrist of the hospital security person, though, as well.

Steve: Well, that's, I mean, this is a very good point, is the fact that she was going to a public email service, downloaded and installed this thing. Who knows what the actual protocol was for it. But clearly it's packaged so that it will get itself installed in exactly the scenario you want to - to the degree that you want it installed anywhere, you want to be able to control where it's installed. And this spyware was invited into this hospital's pediatric cardiac surgery department and created problems for everybody.

Leo: Not so good.

Steve: Not so good.

Leo: Not so good.

Steve: I did want to mention that there is an unpatched vulnerability in Microsoft's SMB version 2. SMB is the Server Message Blocks protocol. It's the general Windows file and printer sharing protocol which is used now for, like, much more than just file and printer sharing under Windows. Their newer version, which appeared first in Vista and is also in the current pre-release of Windows 7, has a known vulnerability which has not been patched. Now, I doubt that this is really a problem for anybody because for this to be a problem you would have to have that port, ports 139 and 445, which are the default ports for this service, or actually the only ports for this service, you'd have to have them open and exposed to bad guys, which would mean you'd have to have them deliberately open through the firewall running on the Windows machine. And assuming that you're behind a router, you'd have to have those mapped through so that you could access those ports and this SMB service remotely. So that seems unlikely to me.

But it's certainly possible that somebody running Vista could have said, oh, well, I've got a really good password and username on my machine. It's crucial for me to be able to do file sharing or printer sharing remotely. So they may well have mapped these ports through. So if that's the case, I wanted to point people at a Microsoft security advisory. There is no patch for this. But you can disable in the registry only the v2 enhancements. And that's where the problem is. So if you were still doing and needed to do this unwise thing of leaving those ports openly exposed, I mean, these ports have been a disaster from day one of Microsoft's platform on the Internet. I mean, it's...

Leo: Isn't this how you got into the whole business?

Steve: Yes. It what brought me into Windows and Internet security. And it's why I created ShieldsUP! was to bring an awareness of this so...

Leo: People had their filesharing ports, just everybody had it just turned on.

Steve: Yeah.

Leo: And it was just - you could see everything.

Steve: There were no personal firewalls. This was pre-router. This is when, god help us, people just plugged their Windows machines directly onto the Internet.

Leo: Look, I can print from anywhere.

Steve: Oh, yeah, look at that.

Leo: Look at that.

Steve: People's printers would, like, be spitting out random spoof pages because somebody thought, oh, this will be fun, we'll print on this random machine that's been exposed. So anyway, Security Advisory - god help anybody who's doing this, but just for the sake of informing everyone - Security Advisory 975497.

Leo: Okay.

Steve: Again, that's 975497. If you have to have these ports open, if you refuse to use a VPN, OpenVPN or something, if you - even port filtering. You should, for example, I mean, I have these ports exposed, but they're locked to the IP address of respective networks so nobody can see them. They're absolutely nonresponsive. It's only when you are at the IP that is permitted that there's any acceptance of packets. And they can't be spoofed because these are TCP connections. So my system is super tightly locked down. But it is possible to filter these so that you're only able to see these ports from a known

IP or range of IPs, which is very good, strong security. But just having it wide open, it's like, okay, well, you get what you deserve. But it is possible at least to disable v2 using this security advisory. And I would absolutely recommend it.

Also I just wanted to mention the blurb in the news recently, Leo, about the FCC's proposed actions on the issue of Net Neutrality.

Leo: Okay, yes, because Monday the FCC announced this. Julius Genachowski said we're going to impose rules requiring this.

Steve: Yeah, it's apparently a contentious issue. I can't remember the name of the female senator, the Republican senator from Texas...

Leo: Kay Bailey Hutchison, yeah.

Steve: Kay Bailey Hutchison has already introduced legislation to block this. So we've never talked about Net Neutrality. Doesn't really bear on security. So it's like, eh, okay, that's sort of off topic for us. But it is something that continues to surface over and over again. You remember that back in the day, as they say, this was an issue with AOL because people were hooking up to AOL and leaving their telephone connections up 24/7, often for days or weeks at a time. And the argument was that AOL was getting a free ride on the carrier's connections. Basically the phones were never - phone lines were never meant to be used this way. And so the issue was, well, wait a minute, how is this fair for some users of the phone system to make a free local call in perpetuity, essentially, tying up this system, using it in a way that was really - it wasn't designed to be used for. And the argument was, of course, that AOL was getting a free ride on this transit that was owned by other public utilities.

And so here we are again looking at these same issues as companies like Google and Microsoft are, the argument goes, trying to take unfair advantage of the broadband services by causing them to be used in a way that they weren't designed to be. And of course the EFF and proponents of Net Neutrality argue, wait a minute, it's fundamentally wrong for some services being carried over the Internet to be charged differently than other services. It ought to just be kept neutral. So, you know.

Leo: You know, it's funny, we were talking about it on TWiT a little bit. And Dvorak was saying...

Steve: I would have loved to have heard John rant.

Leo: Well, I'm a, you know, I believe in Net Neutrality, especially if you've - part of the problem with it is the name. It really should be phrased "antidiscrimination on the 'Net," and then it makes a little more sense to people. We're talking about not discriminating, preventing discrimination on the 'Net.

Steve: Well, and for example, not rate limiting certain types of traffic.

Leo: Right.

Steve: Where we've seen ISPs dropping connections that they determined were bulk file-sharing connections.

Leo: But Dvorak pointed out, and it's true, that there are arguments on both sides. And one of the arguments against it is that you're making a regulation to fight something that's not really happening. And I'm sure that Kay Bailey Hutchison's point is, well, the market should really determine this, not the government. The problem is we don't really have real competition among Internet service providers. In many areas you only have one or two. So you don't - there is no market.

Steve: Right. I've got Cox Cable. Like it or not, that's my cable supplier.

Leo: Right, right. So on balance I think it's the right thing to do. I can understand why people say, oh, do we need another government agency, another...

Steve: More regulation.

Leo: More regulation. But I think that it's probably a good idea to at least put a flag in the sand and say, you know, you can't do this, guys.

Steve: Well, and maybe just lay down some guidelines.

Leo: Right, what can you do, yeah.

Steve: For the FCC to say, okay, look. Here's the status of this argument. This is what we think about it.

Leo: Yeah, yeah.

Steve: I just want to briefly mention, many people have written asking what's going on with me and my Vitamin D blood levels.

Leo: Yes.

Steve: And what I learned from literally testing every single week was the variation in the testing accuracy was completely masking what was going on. So it was annoying. Basically I was testing too often. It's a little bit of a misnomer. The results come back with one decimal point. So it's like 22.2, 29.7, as if that decimal point had any meaning whatsoever. What I saw was that from week to week there was, like, a plus or minus 5, I would guess, variation. I mean, like, as in 5.0. So this notion of giving me three digits of accuracy was ridiculous. And it was chewing up my arm in the process, too.

So I just decided I would be checking in monthly to see what was going on. We never did tell our listeners that because there was some reason to believe that it was wrong to bathe immediately after coming in from the sun, because you'd literally wash the Vitamin D that had been synthesized in your skin out of your skin, that I also did the experiment of deliberately not bathing, not showering at all with soap for a week to see if that made any difference. And the fact is, it was after that week that I was, for the first time ever, no longer deficient in my Vitamin D level. But that wasn't even - that wasn't clear with any scientific accuracy because the next week I was.

So there's a huge variation in the test. It's very inaccurate, or relatively so. So I will, over the course of a much longer baseline, be checking now only every four weeks. And I'm going to be checking at the end of the month to see where I am. I am now supplementing. The whole put-me-in-the-sun thing was just to see whether I could get - just to see the effect of being in the sun. And unfortunately I wasn't willing to do that over the course of month after month after month. I thought, well, if I could do it over the course of a few weeks, that would be fun. But it's hard for me to hold still for half an hour.

Leo: I can imagine. All that coffee inside you, for one thing. No, I'm glad to hear that. I've been supplementing with D ever since. I just think it's not worth taking a chance on that one.

Steve: Oh, I agree. In fact, I had set up - I wanted to read a couple letters that were just anecdotal, and I want to say evidence, but they're not evidence. They were just anecdotal events which argue about the pro-immune system effects of D. It's sort of on people's radar as we approach wintertime and this H1N1 'flu concern. And of course the anecdotal evidence is that D is very good for your immune system. And there was a clinic where, I think it was in Wisconsin, where during an H1N1 'flu spike there were two doctors in a clinic. One who wrote the letter had all of her patients on D just because she was in Wisconsin - I think her name was Ellie. She was in Wisconsin, and she believed that D was important. The other doctor with whom she shared this clinic wasn't D-aware and wasn't doing anything.

During this spike they were once having coffee, and he commented that one out of ten of his patients had been tested positive for H1N1, and none of hers. Zero. So again, that's not scientifically accurate, I mean, it doesn't prove anything statistically. But I'm more of an expert on statistics than I was last week before I wrote all this new code for the DNS benchmark. But again, it's another data point on the radar. I'm glad I'm aware of this, and all my friends and family are now. And everyone's taking their little - I call it the little drop of sunshine.

Leo: Yeah, yeah.

Steve: But it's a little yellow capsule of olive oil, basically. And I did have a really fun SpinRite success story to share. I love it when a letter that we receive starts out, "Wow, what a product."

Leo: Always a good way to start.

Steve: Wow, what a product. Justin, who didn't give me his last name, wrote. He says, "I've been an administrator off and on for the past 12 years." And he - I guess he means IT administrator. "So I've seen a fair share of crashed hard drives. I've seen how much money it can take to restore valuable data, and it's never cheap," he put in all caps. He said, "My uncle called me a while back to see if I could maybe get some data off his crashed hard drive because he did not have the money to have it professionally done. The drive sounded like it was a tin can of nuts and bolts when it ran," which really sounds quite frightening. And he says, "And I told him it was unlikely that I would be able to do anything with it. I got estimates from a few of the big name hard drive restoration companies, and the total was to be in excess of a thousand dollars, no matter who I talked to, and with no guarantee of success.

"I've heard of your product before, but for whatever reason I just didn't imagine that it could resolve the problem this drive was having. But last night I figured, what the heck. So I purchased and downloaded your product and easily created my boot disk and was quickly underway to see if this crashed drive could be accessed just one more time." Of course, that's what everybody wants. It's like, oh, my god, I'm sorry...

Leo: Just once more, yeah, please.

Steve: Just [indiscernible] to me one last time.

Leo: One more time.

Steve: I promise I'll get all the data off I need. So he says, "It took 14 hours to complete the task because of how bad of shape the disk was in. As a matter of fact, as I watched SpinRite's progress screen and noticed all of the bad sectors that it was turning up, I just knew that it was worth a shot because there was no way" - well, he says, "I just knew that it was worth a shot, but there was no way I'm getting data off of this drive. Well, as I write this now, I'm copying all of the wanted data off the old drive, onto a new drive! I am absolutely amazed that this worked on a drive that sounded the way this one did. And for 90 bucks? Too cheap. This drive was barely even recognizable in the system BIOS, much less accessible in Windows. Windows would freeze just trying to boot off a good disk while this bad disk was attached as a secondary. That's how bad this disk was messed up. It would mess everything else up. Thank you, guys. My uncle will now have all of his data returned, most of which was irreplaceable pictures of his family, children and grandchildren, et cetera, et cetera, data that is priceless. Good job. Justin."

Leo: Fantastic.

Steve: Yeah. Love it.

Leo: That's a nice - that's a nice story. I like that. All right, Steve, I'm ready. I've got security maxims all queued up.

Steve: These are great. I think, as I said at the top of the show, they're compiled by a guy who's been living and breathing security for a long time. We'll find some references to a well-known cybersecurity guru, Bruce Schneier, in here.

Leo: Love Bruce, yeah.

Steve: And there's a - I think what these reflect, as we'll see as we go through them, is a philosophy that many of our listeners I'm sure have grown to understand and probably even adopt. From all the feedback that we get, when people say I aced my security exam, I've learned more about security from the podcast than I did in college, blah blah blah, I mean, there's a - it's sort of hard to describe, but a clear, discernible approach which I guess for lack of a better word involves skepticism about the assumptions of things being secure.

Leo: Well, that's your maxim, Trust No One.

Steve: Yeah, TNO is - exactly.

Leo: That's all you really need to know. That's the starting point.

Steve: That's a good starting point. And we'll see that reflected though these, also.

Leo: Well, let's start with Maxim #1, the Infinity Maxim. You want me to read it, or...

Steve: Yeah, why don't you, and then we'll comment.

Leo: Okay. So again, these are from Roger Johnston, who is a CPP at the Argonne Vulnerability Assessment Team, Nuclear Engineering Division, Argonne National Lab, DOE. This guy protects us and protects those nukes. So I'm glad...

Steve: Yeah.

Leo: I'm glad he's [indiscernible].

Steve: These are sort of his pithy distillations of fundamental truths about the nature, the fundamental nature of security.

Leo: Infinity Maxim, and you kind of referred to this earlier, there are an unlimited number of security vulnerabilities for any given security device, system, or program, most of which will never be discovered, either by the bad guys or the good guys. Now, should I read his comment, too? Or is that...

Steve: Yeah, I think his comments are normally good, too. So, yeah.

Leo: All right. I'll include that. We think this because we always find new vulnerabilities when we look at the same security device, system, or program a second or third time, and because we always find vulnerabilities that others miss, and vice versa.

Steve: And you're right, I think; so this is his Infinity Maxim, meaning that everything is insecure basically.

Leo: Nothing's secure, yeah.

Steve: Exactly, that fundamentally, the closer you look, the more you find. And so the presumption of security - it's a little bit about I think there's - certainly we see all around us instances of denial. It's easy to say, oh, yeah, we got security, mostly because we want to say we've got security. And so it's hard to argue until you hold up in someone's face where there's a problem, and they go, oh, okay, we'll just fix that, and now we've got security. Eh, no. Let's look some more, and we'll find some more problems.

Leo: It's not exactly a mathematical proof. But it does, it kind of stands to reason just empirically that every time you look, you find another one.

Steve: Maybe it's that, like from a standpoint of entropy, randomness, it's more difficult to construct than it is to destruct.

Leo: Yes.

Steve: That is, it's much more difficult to order and organize than it is to disorder and disorganize. And breaching security, breaking security is fundamentally about destroying something. It's about bringing randomness back to a system that was trying to be ordered against it. And so it's fundamentally an uphill battle.

Leo: Yeah, yeah. Impossible. Maxim #2, the Thanks for Nothin' Maxim. Thanks for nuttin'. A vulnerability assessment that finds no vulnerabilities, or even only a few, is worthless and wrong.

Steve: I like the "Thanks for Nothin'."

Leo: Thanks for nothin'.

Steve: So someone says, okay, I want you to assess our security. And they come back and say, ah, perfect, you've got perfect security.

Leo: That's not what I want to hear.

Steve: Thanks for nothin'. How much did we pay you for that?

Leo: It's perfect. There is no such thing. The Arrogance Maxim: The easy of defeating a security device or system is proportional to how confident/arrogant the designer, manufacturer, or user is about it, and how often they use words like "impossible," as in "impossible to crack," or "tamper-proof."

Steve: Yeah, the Arrogance Maxim, I love that. It's like...

Leo: Yeah, it's so true.

Steve: Well, and it's funny, too, because if you listen to the words that security people use, like if you listen to the way Bruce Schneier talks, I mean, he'll never - you couldn't make him say, no, it's invulnerable, or there are no vulnerabilities. Always the word "known" is there, no known vulnerabilities. There's nothing that we know about it that is vulnerable, or currently vulnerable or, well, we know what the theoretical problem is, but it's unlikely before the universe ends that that will be a problem. I mean, there's always a caveat because, if you're security aware, you recognize that, I mean, the reality of the need for lack of arrogance. I mean, arrogance will get you in trouble faster than anything else.

Leo: At best, I mean, it's probabilistic. At best you could say there's a probability that it's secure. That's the most you could hope for. And you do that all the time. I'll try to pin you down and say, well, this makes it secure; right? And you'll say, well...

Steve: More secure.

Leo: More secure.

Steve: Or maybe.

Leo: Maxim #4 ties right into that: Be Afraid, Be Very Afraid. If you're not running scared, you have bad security or a bad security product. And his comment is fear is a good vaccine against both arrogance and ignorance.

Steve: Yeah, I think that's a very good point. I mean, while I am coding CryptoLink, there will be nothing on my mind more than the fear that I'm going to make a mistake. I mean, I'll be about as far away from arrogance as I could imagine. I'll be looking at every single thing I do, line of code, algorithm, protocol, just like I hope, I hope, I hope this is right. Yeah.

Leo: Well, this is almost a corollary then. The So We're in Agreement Maxim says, if you're happy with your security, so are the bad guys.

Steve: I love that. That's great.

Leo: Ignorance is Bliss Maxim: The confidence that people have in security is inversely proportional to how much they know about it. It's true. Doing this show has made me much more scared than ever before. And his comment is, security looks easy if you've never taken the time to think carefully about it.

Steve: Yeah. And I think if anything else, you're right, Leo, that's what this podcast over the years has helped to imbue our audience with is this, again, ignorance was bliss. They're no longer ignorant. And now they really have a much greater appreciation for how hard security is.

Leo: Yeah. Sometimes, though, you kind of wish you could go back. Everything's safe.

Steve: Exactly. It was just nicer. You could sleep at night.

Leo: It's all fine. Everything's going to be fine. Here's the Weakest Link Maxim: The efficacy of security is determined more by what is done wrong than by what is done right. He says the comment here, because the bad guys typically attack deliberately and intelligently, not randomly. Now, you're going to have to explain this one.

Steve: Well, a perfect example we talked about a few weeks ago with the vulnerability that was found in the use of the MD5 hash which was used to sign the security certificates for SSL. So the point is, there was this little, tiny, really hard to deal with or to leverage, microscopic flaw in this powerful, sophisticated, interlinked, beautiful technology for guaranteeing the identity of someone you were connecting to. And because the guys who were attacking this managed to come up with a way that they could control some aspect of a slight defect, I mean, arguably, okay, this is not a problem defect. They've turned it into one. So the weakest link in this whole chain brought the whole thing down. It really is the case. It is, unfortunately, no matter how good the security of your entire system is, the bad guys are looking, and as he points out in the comment, not randomly, but they're looking for some entry point, the weakest link. And that weakest link determines the security of the entire system. And again, it's another example of why this is just so fundamentally difficult.

Leo: Yeah. That makes sense.

Steve: It's not like, well, it's not fair. We want it to be the average security.

Leo: Right, right.

Steve: It's like, sorry.

Leo: We worked so hard on this.

Steve: Yeah. Doesn't work that way.

Leo: We did almost everything right. High-Tech Maxim: The amount of careful thinking that has gone into a given security device, system, or program is inversely proportional to the amount of high technology it uses. So in security, apparently, high technology is often taken as a license to stop thinking critically.

Steve: I think that's really interesting. It's like, now wait a minute, we have geometric folded space quantum entanglement encryption. It's like, uh-huh, but didn't you leave the back door open?

Leo: But it's high tech. It's high tech.

Steve: Exactly. Sometimes this notion of, like, using all this fancy stuff, and it's like, oh, look how fancy that is. Look at all the little blinky lights, all those lights...

[Talking simultaneously]

Steve: Just get a big padlock.

Leo: That's kind of a universal thing, you know, in society. Oh, it's modern. It must be better. Oh, it's high tech, it must be better. Oh, it's digital, it must be better.

Steve: And frankly, we're all stuck on this, I mean, I chastise myself for wanting the latest version of the software.

Leo: Yes.

Steve: I mean, we're always - we're sort of feeling like, oh, maybe the next one will be better, hoping that it's like it won't hang or it won't crash. I don't even mean security flaws. I just mean there's this - we're stuck on this gravy train of updates, wanting the latest and the greatest, thinking that the latest is the greatest.

Leo: Yeah. Boy, that's exactly it, isn't it. Latest does not mean greatest. In fact, in security it's the opposite.

Steve: Yeah, I'm using...

Leo: Mature means safer.

Steve: I'm using Studio 7 of Pinnacle for video editing, even though they're at 12 or something...

Leo: They are at 12.

Steve: ...because it was the best. And I'm using an old HP, not 35, an HP-21, I think it is, the old scientific calculator, which is really old now. But it was the best. And Paint Shop Pro, I use version 5, I think, which is like - because they went too far. They added too much junk to it, and it slowed it down, and it became a problem. So, like, okay, no. I'm just going to stay with what I have.

Leo: That's often true in software, isn't it.

Steve: Yeah.

Leo: Maxim #10, the Dr. Who Maxim. It's in quotes, so I'm thinking this must be a quote from Dr. Who.

Steve: Yes, it was.

Leo: "The more sophisticated the technology, the more vulnerable it is to primitive attack. People often overlook the obvious." It's like the Death Star. There was this one...

Steve: Yeah, that little hole...

Leo: ...little mistake in the whole thing.

Steve: Right, but looking at the size of this planetary attack thing, it's like, oh, my god, what are we going to do?

Leo: And there was one little attack vector.

Steve: Yup.

Leo: This is the Low-Tech Maxim: Low-tech attacks work, even against high-tech devices and systems. Comment: So don't get too worked up about high-tech attacks.

Steve: You know, it's sort of...

Leo: Well, social engineering is often the way people get into stuff. You can spend a lot of time on getting the right algorithm, but then somebody asks you what your password is, and you tell them.

Steve: Or, like, imagine, when I think of low-tech attacks work even against high-tech devices, I think, you know, here's the alarm system, and you just take the batteries out.

Leo: Yeah [laughing].

Steve: It's like, oh, whoops. All fancy, but now it's just powered down.

Leo: Oh, these are so good. This is refreshing because it really - it reminds us of stuff we always have known, but you just forget.

Steve: Yup.

Leo: Or of things that you do unconsciously that you really ought to remember. Maxim #12 he calls Schneier's Maxim #1 or, a.k.a., the Don't Wet Your Pants Maxim. The more excited people are about a given security technology, the less they understand, one, that technology; and, two, their own security problems. Comment...

Steve: I thought that was fun.

Leo: Yeah.

Steve: And so the more excited they are. So again it's like, oh, we've got gazillion-bit encryption. Isn't that great? It's like, uh, okay, calm down. That's, you know, maybe better than gazillion-minus-one-bit encryption.

Leo: Right.

Steve: But it's not that clear that this really solves the problem. Or that that is the problem that needs to be solved. You know, we've seen so many examples over the years of really good technology being misapplied, and the bad guys just slip right around it. They're excited because they realize there's a simple way to solve the problem.

Leo: Maxim #13, the Too Good Maxim: If a given security product, technology, vendor, or technique sounds too good to be true, it is. And it probably sucks big-time [laughing].

Steve: This makes me think of all of the ridiculous claims about some random, homegrown encryption algorithm.

Leo: Yeah, yeah.

Steve: And thank goodness we're seeing that less now. But you still encounter it from time to time. Some website will say, oh, my 13-year-old son came up with this amazing encryption technology, and so that's what we're using. It's like...

Leo: Oh, boy.

Steve: Thanks anyway.

Leo: Oh, boy. Maxim #14, Schneier's Maxim #2, the Control Freaks Maxim: Control - oh, I know this one. Control will usually get confused with security. Even when control doesn't get confused with security, lots of people and organizations will use security - oh, this is the corollary. That's Schneier's Maxim, Control Freaks Maxim. And really Johnston's corollary is, even when control doesn't get confused with security, lots of people and organizations will use security as an excuse to grab control.

Steve: Yup.

Leo: Mm-hmm.

Steve: So I love that. It is absolutely the case, that is, this issue of control getting confused with security. Many, many people believe that, for example, bolting things down is a replacement for, or actually equivalent to, security. And it's just not the case. You'll often have, for example, in a corporate environment, the security people being unnecessarily controlling and still having security problems because control doesn't automatically bring high levels of security.

Leo: The TSA leaps to mind here.

Steve: Uh-huh.

Leo: Where, you know, they make you take off your shoes as you go through airport security. I don't know if that enhances security. It enhances control.

Steve: And actually we're going to get to a specific maxim that talks about the security theater and...

Leo: The theater of security, yeah.

Steve: The theater of security.

Leo: Yeah, Bruce Schneier talks about that lot, actually. This is a big hot button for him. Maxim #15, Father Knows Best Maxim: The amount that non-security senior managers in any organization know about security is inversely proportional to, one, how easy they think security is; and, two, how much they will micromanage security and invent arbitrary rules. Another control maxim, yup.

Steve: And again, it's this - there's a problem with senior management that doesn't know anything about security and, consequently, thinks it's easy and doesn't understand why...

Leo: Right. Oh, what's so hard?

Steve: Yeah, exactly. It's like, oh, well, you know, what are you making such a big deal about all this? It's obviously just easy. Just go do your security job. Okay.

Leo: If you were just doing your job, none of this would have happened. This is Big Heads Maxim: The farther up the chain of command a non-security manager can be found, the more likely he or she thinks that they understand security, and that security is easy.

Steve: Sort of the Peter Principle of security.

Leo: Yeah, they rise to the top, don't they.

Steve: Yeah. Love that.

Leo: Voltaire - oh, I'm sorry. I'll get to Voltaire's Maxim in a second. This is the Huh Maxim: When a nonsecurity senior manager, bureaucrat, or government official talks publicly about security, he or she will usually say something stupid, unrealistic, inaccurate, and/or nave.

Steve: Yeah. So that's just nonsecurity people who are being asked security questions, who basically sort of make it up as they go along.

Leo: That leads us to Voltaire's Maxim: Common sense isn't all that common. He says real world security blunders are often stunningly dumb. And in defense of managers, they often come from so-called security experts, too. This can go both ways; you know? It's not just the upper-level people that can do incredibly stupid things. We're all capable of it. We all have a blind spot here or there.

Steve: Yeah, I think that's really true.

Leo: Yeah. And really arrogances can get you in big trouble of thinking, well, I know better than they do, or they're just foolish. Here's the Yippee Maxim: There are effective, simple, and low-cost countermeasures, or at least partial countermeasures, to most vulnerabilities. You think that's true?

Steve: Well, he - okay, now, this, I think, does apply more to the physical security world than to the cybersecurity world. So this is an example of where I would argue that physical and cybersecurity diverge a little bit. So he's, like, thinking, okay, if you've got something really valuable, just stick it in a safe that's secure instead of surrounding it with radar fields and motion sensors and all this where it's all fancy; but it's like, okay, just keep it out of sight, lock it up, for example, in physical security terms.

Leo: Yeah, very straightforward.

Steve: So I think it is very often the case that people get themselves all wound up in very complex scenarios where it's like, wait a minute, you know, your grandmother would have just solved it this way. Oh, yeah, and that works.

Leo: You know, there's a corollary there, the Bond Villain Corollary, where the more complex the device designed to kill James Bond, the more likely he will escape. Right?

Steve: Right. Or that might be the Roadrunner Maxim, also.

Leo: Yes, the Roadrunner Maxim, yeah. Here's the Arg Maxim, and it's not Talk Like a Pirate Day: But users, manufacturers, managers, and bureaucrats will be reluctant to implement these effective, simple, and low-cost countermeasures for reasons of inertia, pride, bureaucracy, fear, wishful thinking, and/or cognitive dissonance.

Steve: And I might add to that list, or previous investment.

Leo: Yes.

Steve: It can very often be that people become invested - and I guess that would be inertia and pride. They become invested in a particular solution, and someone comes along and says, yeah, but just do that. It's like, oh, no, no, no, no, we have - this is version 3, and we paid a lot of money for this. So that's what we're going to use.

Leo: You know, we've gotten through 20, which is only half of this first chunk. Maybe it would be a good time to stop here because I don't want to use them all up. These are great. And I also don't want people to get in a blur about all of them because they're so good, it's kind of good to think about it a little bit.

Steve: Perfect. Let's - we will hold the balance for a future episode, Security Maxims Part II.

Leo: 20 security maxims from Roger Johnston, who deserves a lot of credit for these. But I tell you, anybody who's worked in security, I just can hear their voices. They know these. These are well known by people who've had to deal with this for a long time. And it's good to share this with the rest of us.

Steve: Well, it's funny, too, as I'm scanning ahead and thinking, oh, okay, I can't wait till we get to the other ones, so...

Leo: Well, we're going to have to do this again.

Steve: We'll do that again.

Leo: Steve, always a pleasure. Steve Gibson is the author of a great program for hard drive maintenance and recovery, SpinRite. You must have this. Go to GRC.com, that's his website, and get a copy for yourself. And you know what I told somebody on the radio, and I just want to make sure I didn't say this incorrectly, he was having a problem that really sounded like a SpinRite - that SpinRite could solve it. And but I said, you know, there are a variety of problems you can have. There's hardware problems. SpinRite's not a - can't fix a broken, busted head or frozen bearings. And then there are file system problems. SpinRite doesn't really work at the level of the file system. So but it sounds like this guy had just kind of classic symptoms. I said it sounds like SpinRite's going to do it. But I told him you have a 30-day money-back guarantee, do you not?

Steve: No. It's no day limit.

Leo: Unlimited money-back guarantee.

Steve: It really is. I mean, I don't ever want...

Leo: You should make it 30 days.

Steve: I don't ever want anyone to feel like they made a mistake buying SpinRite. And so I don't want anyone - I would not want anyone's money who...

Leo: That's perfect.

Steve: ...thought that they regretted their purchase. I mean, we don't have a demo because there's really no way to demo it. It fixes the problem when you run it.

Leo: You're done. The demo's done. Right.

Steve: Yeah. So I didn't want to have it, like, time limited or expiring or anything. So instead we just give you your money back. If for whatever reason, with no questions asked, you're not happy, we'll give you your money back.

Leo: Well, good. That's what I told him.

Steve: And not even 30 days. I mean, maybe five years would be pushing it a little bit.

Leo: We had a - didn't you - we had a guy a couple months ago or a couple weeks ago who said, yeah, it was like five years later. Yeah, there's a limit. That's why I said 30 days. But anyway. You could try.

Steve: It's really, again, I would not want any - I would never keep anyone's money who wasn't happy with SpinRite.

Leo: Doesn't work for you...

Steve: We'll guarantee your satisfaction.

Leo: ...your money back.

Steve: Just a flat-out satisfaction guarantee. And most of the time, I mean, we've run across situations that seemed to be file system related. There was one just the other day where it wouldn't - some customer reported that he had to soften chkdsk's running by doing a /i option on chkdsk, which told it don't check the indexes, the NTFS file system indexes so closely. And he said, you know, do you think - does that sound like something SpinRite would fix? And I said, you know, technically no. But I'm always surprised by, literally, I mean, as the author I'm surprised by what SpinRite does. It surprises me. So I guarantee you that, if it doesn't fix it, you can have your money back. And he wrote back later, he says, well, I don't know why, but it fixed it. So I go, okay.

Leo: Well, what it tells me is that most of the time the problems are hard drives' bad sectors, as opposed to a cosmic ray hitting the file allocation table or the index tables or, you know...

Steve: Well, yes. And especially with the NTFS file system. It is a file system that has a lot of redundancy in it.

Leo: Ah.

Steve: So it's not like the FAT file system that was always getting lost clusters. Remember the old lost clusters problem.

Leo: Oh, horrible, horrible, yeah.

Steve: And so the FAT file system tends to be structurally more robust. So you don't often have structural problems unless they are caused by physical problems.

Leo: Right.

Steve: So when you fix the physical problems, what looked like a structure problem gets fixed in the process.

Leo: That's why it's worth trying. GRC.com. And while you're there, by the way, check out ShieldsUP!, all the free programs Steve offers. He's very generous with his time and his software. Some great stuff on there. And of course the great security forums. In fact, we'll be doing questions next week. So if you want to leave a question about anything we talked about on the show, or something you've heard, you can go to GRC.com/feedback and leave a question there. We'll get to some of your questions in the next episode. Steve, always a great pleasure.

Steve: Talk to you soon. Actually, talk to you next week.

Leo: Next week, on Security Now!.

Steve: Okay, Leo. Thanks.