SECURITY NOW!

Transcript of Episode #553

Too Much News

Description: Leo and I discuss a VERY interesting week of news: The FBI dropping its case against Apple, claiming not to need them any longer; a distressing possible smartphone encryption law for California; TrueCrypt's origins; a Certificate Authority horror; more hospitals hit with ransomware; a bad flaw in the SMB protocol; finally some good news on the IoT front; GRC's new Never10 freeware; and a discussion of the monster PC I just built.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-553.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-553-lq.mp3

SHOW TEASE: It's time for Security Now!. We're going to talk security big-time. Lots of news this week. And we'll talk about Steve's new utility, Never10 - Never10 - and his brand new PC build, which is mindboggling. I asked him how much it cost. He said, "I don't know, I didn't bother to add it up." I wouldn't, if I were you, Steve. It's all next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 553, recorded Tuesday, March 29th, 2016: Too Much News.

It's time for Security Now!, the show where we cover your security and privacy online with the Explainer in Chief, Mr. Steve Gibson from GRC.com. And a happy day to you, Steve. I'm sorry I wasn't here last week, but I hear you and Father Robert Ballecer had a wonderful time together.

Steve Gibson: We had a good time, and we broke the all-time podcast length record last week. We went over 2.5 hours. You and I have been a little bit on the high side of two hours most recently, and that's about where I want to be. Elaine likes it because I pay her by the podcast minute. So back when we were doing 20-minute podcasts, Elaine was very affordable. Now we're at 2.5 hours, and it's like, okay, well, I am occupying a lot more of her week. But I'm glad to have the transcripts, so it's a win. Anyway, last week we talked about the DROWN attack. And I thought about doing a Q&A except that there's no way, with everything that is going on this week, that there's time to cover a Q&A and all the news. So this is just one of our too-much-news podcasts.

Of course, big in the news is the FBI dropping its suit against Apple, saying that they don't need them. There's an interesting and distressing Assembly Bill going through the California State Assembly. We've got some news just this morning about apparently what very much looks like the origins of TrueCrypt.

Leo: Good. I was hoping you were going to talk about that one. That's good, yeah.

Steve: Yeah. A blood-chilling flaw in a Certificate Authority has been found. Two more hospitals hit with ransomware.

Leo: Oh, no.

Steve: And unknown problem with the Samba protocol. Some good news on the IoT front, finally. And of course I introduced, late last week, a new piece of freeware that I will talk briefly about, just because a lot of people have been interested. I want to also not forget to thank Paul and Mary Jo. They both immediately covered it on their respective outlets, so I really appreciated that.

And then I built, as I've referred to it several times over the last couple months, I built a monster PC to replace the one I'm using. The one I'm using is getting a little creaky. It is a 32-bit XP, and so just the RAM ceiling is a problem. So I needed to go to 64 bits. I wanted to go to Windows 7. But normally I would wait except that, I mean, the system I've got is fine. It's been running for years. In fact, just until recently it had been on SP2 of XP because it never kind of liked SP3. But I had to bite the bullet a month ago and move my XP up to SP3 in order to get it to understand SHA-256 certificates. So now I'm on SP3 of XP, which is a brand new thing.

So obviously I'm lagging a little bit behind. But I was worried that we were going to lose compatibility with future hardware for Windows 7. And I don't - I think I want to stay with Windows 7 for the foreseeable future. And, I mean, you know, foreseeable future for me means a 10- to 15-year horizon. So I needed to get hardware now that Windows 7 worked on because Microsoft has said that they're not guaranteeing that they will, I mean, and it's understandable, Windows 7 is getting old. Why should Windows 7 necessarily run with hardware three or four generations from now?

So that was the impetus to get the state-of-the-art hardware today to use for my replacement machine. The point is that lots of people have wanted more details than I've provided. So at the end of the podcast I've got - the show notes also broke a record this week, 1MB show notes, because I have four large high-resolution photos inside the case of my machine at the end of the show notes, for anyone who wants to see. And we'll do it at the end of the podcast so that people have no interest whatsoever can hit stop and go on to the next TWiT podcast, rather than listening to me talk about the machine I built. So lots to talk about.

Leo: Yeah, no kidding. All right. Let's dig into it here, Steve.

Steve: So I'm sure you must have talked about it on MacBreak Weekly, and unfortunately I wasn't able to listen to the beginning of that previous podcast. I was busy running around and getting this all put together. But the big news is that the U.S. government, in a filing, dropped its case against Apple. And so the Picture of the Week on the first page of the show notes is a snapshot of the very brief two short sentences that were filed, that reads: "Applicant United States of America, by and through its counsel of record, the United States Attorney for the Central District of California, hereby files this status report called for by the Court's order issued on March 21, 2016." And then it ends with "The government has now successfully accessed the data stored on Farook's iPhone and therefore no longer requires the assistance from Apple Inc. mandated by Court's Order Compelling Apple Inc. to Assist Agents in Search dated February 16, 2016."

Now, what's interesting about this is that there's a lot that isn't being said because the FBI has no obligation to inform us of, quote, "ongoing investigation" is always the way they get out of - oh, you know, we don't comment on ongoing investigations. So they're able to just say by policy they're not going to say anything more. But what was really interesting is that the coverage of this is, some of it, and some of the best of it, is questioning what they actually got. And the best piece of it was a video on "The Today Show" this morning where Pete Williams, who's the NBC reporter, and a very careful, meticulous reporter...

Leo: He's their DoJ guy? He was their Pentagon guy.

Steve: Yes. Pete Williams is also the main legal guy they go to whenever the Supreme Court does any sort of a ruling. You know, they bring him out to explain what this all means. So he stated that officials say that the data they extracted from the phone is encrypted and will take some time to decode.

Leo: Oh, that's interesting.

Steve: It really is interesting. And they haven't, the FBI has not said they have decrypted it. They have said they have extracted the phone's data. Well, okay. That's not hard. In fact, we talked about it last week or the week before. One of the presumptions the guy who...

Leo: Do you think he got it right, or he just - I mean, is that credible?

Steve: See, that's just it. I trust Pete. And if the government said - if he says that government officials told him it is still encrypted, then, I mean, that's the best reporting I've seen.

Leo: Yes, yeah, yeah.

Steve: And he stated it in public on "The Today Show" and has been quoted. I had a link to a little...

Leo: See, that isn't what they - see, but the reason I question it is that isn't what they were asking Apple to do. Because what they were wanting Apple to do was make it possible for them to decrypt the data.

Steve: To unlock the phone.

Leo: Which would, in the process of unlocking it, decrypt the data.

Steve: Correct.

Leo: So I don't buy it because, if they really only had encrypted data, A, we know it's going to be impossible for them to decrypt it.

Steve: Correct.

Leo: And, B, it doesn't satisfy their need, their demand, in which case they wouldn't have had to withdraw - I think they only would have withdrawn this because they had to, because the law says the All Writs can't be used if you've accomplished the goal. But they didn't accomplish the goal. So I'm going to call BS on the statement. Whether Peter misstated, or whether he was told something incorrect, that can't be right.

Steve: It can be right, if the alternative theory is that the government knew they had a weak case. They were bringing some witnesses into the hearing. Readers of this believe that the fact that the FBI was bringing witnesses in meant that they knew they had a weak case. And they may have chosen not to push this and lose on the All Writs Act issue and instead say, oh, don't worry about it, we've got the problem solved.

Leo: Yeah, but, no, they're not going to lie in that affidavit to the court. I mean, I think they would be very unlikely to lie and say we no longer need Apple's help, when in fact they don't have the data. They're not going to pull it, they can't just pull it because they feel like, oh, we're going to lose this case, if they say, as they did, we got it.

Steve: "The government has now successfully accessed the data stored on Farook's iPhone." So that doesn't say we've decrypted it. It says we've accessed it. So anyway, I guess my point is we don't know. And I'm happy with not knowing because there's no way we can know. But I also, I've been following Pete for a long time, and he made it very clear that this data is still encrypted, and they have yet to decrypt it. So I don't know...

Leo: Is there any chance of them decrypting the data?

Steve: Okay. So of course we know about...

Leo: Unless Farook used Monkey123 as a - but there is no passcode; right?

Steve: We know about Cellebrite and the relationship they've had with those guys. We assume that McAfee has not provided any useful input into this process. I mean, and there are some theories. One theory of this, and Jonathan Zdziarski has been proposing this, and that is they could clone the nonvolatile memory to essentially a backing store, you know, back it up; then do their 10 guesses and see whether they're able to get it right. If they don't, then in this theory they're able to restore from their copy back to the phone and try 10 more. That doesn't work, restore again, try 10 more.

Now, the problem is, and the real issue is, we don't have schematics of the iPhone. We don't know precisely where things are. So, for example, is the symmetric key, which we know is necessary to apply to the symmetric crypto, the hardware crypto that encrypts and decrypts the data to and from the memory, we don't know exactly where it is. We assume it's in the Secure Enclave, which is part of the processor. And because it's been, remember, there's been some pie-in-the-sky talk about etching the top off with acid and then using lasers to read the data out and other really low probability approaches to succeed.

So the problem is, you know, I like to know what I'm talking about, and in this instance all we can do is report on the information that's out there. And my feeling is we don't know yet for sure that they've decrypted this, given that a reporter with good reputation has said he was told it is not decrypted. And we haven't ever - nowhere else have we had it definitively indicated that it was decrypted. I would say we don't know.

And of course then the question is, even if they did decrypt it, is there anything useful on it? And there's been a lot of back-and-forth in the industry, of course, about all this. And my sense is Apple knows, there's nothing that Apple does not know about their phone. And they know what the FBI was asking. Absent any flaws - and of course Apple keeps trying to keep their phone from being jailbreakable, yet it keeps getting jailbroken. So there are flaws that Apple doesn't have control over.

But my sense is Apple is going to continue their forward march to make this thing increasingly locked down so that they would not be able, for example, to respond in the same fashion that the FBI just asked them to respond to at some point in the future, that they will take additional measures, like for example the phone won't update unless you unlock it. If they did that, then that forecloses this background update loophole that allows them, as you pointed out a couple weeks ago, Leo, to install any kind of update that they might want to that would alter the phone's behavior and make it possible. So anyway, interesting additional chapter with lots of unknowns in this Apple versus FBI case.

Leo: I'm really curious if the FBI will reveal to Apple, we may never know if they do or don't, the exploit. Because of course what now the FBI has done is let America know, well, there's a way in. There's a flaw. And, I mean, given the FBI's stance so far, I doubt, I mean, I'm sure they would prefer to keep that flaw secret so they could continue to use it.

Steve: Right.

Leo: I can't - I feel like we just haven't heard the end of the government's demands for backdoors. I just...

Steve: Oh, Leo, you could not be more correct. You are absolutely right. And in fact that takes me into the second topic, which is a recently updated California Assembly Bill, AB-1681. There was on the books a law which already required smartphones manufactured on or after July 1 of 2015, so that's last summer, to include a technological solution at the time of the sale which could consist of hardware, software, or both, that once initiated and successfully communicated to the smartphone could render it inoperable. So that was like a remote shutdown which I guess, I mean, if this law is on the books - do you know about that? There's like a remote kill for smartphones?

Leo: Yeah, that's been around for a while, the kill switch.

Steve: Right, right, that's what I thought. And so this legislation updates that existing law.

Leo: That law's been in effect almost a year, I guess, since last year.

Steve: Right, right. Okay. So what this does is this law is being updated. It was introduced on January 20th, then amended on March 8th and corrected on the 18th, so just recently. And so this has been added to Section 22762 of the Business and Professions Code relating to smartphones. And so in the Executive Summary they say of this amendment: "This bill would require a smartphone that is manufactured on or after January 1, 2017, and sold in California, to be capable of being decrypted and unlocked by its manufacturer or its operating system provider. The bill would, except as provided, subject a seller or lessor" - the language is a little mixed up here because I copied it directly out of - "seller or lessor would subject a manufacturer or operating system provider that knowingly failed to comply with that requirement to a civil penalty of $2,500 for each smartphone sold or leased.

"The bill would prohibit a seller or lessor manufacturer or operating system provider who has paid this civil penalty from passing any portion of the penalty on to purchasers of smartphones. The bill would authorize only the Attorney General or a district attorney to bring a civil suit to enforce these provisions. This bill would make findings and declarations related to smartphones and criminal activity." Well, it says "and criminal activity."

Anyway, that's the summary. So this is what we've been expecting. I don't know, I mean, this isn't signed into law yet. I haven't looked at where this is or what it means. Also, January 1st of 2017 is very soon. If this happened at all, I wouldn't be at all surprised to see it pushed back. But this is the kind of legislation that we're expecting to see. The Burr-Feinstein bill still hasn't shown up in the Senate, although it is being passed around and talked about. But I've yet seen no text of it.

And from what little I've gathered, reading every story that I could find, it doesn't seem very sharp. It sort of sounds a little bit like it's sort of blunt and leaves enough wiggle room that it's not clear how people would respond. But this California law, if it ever happened, I mean, is ultimately what I've been predicting, unfortunately, and that is that it would just simply be a requirement that smartphones be able to be decrypted.

Leo: Yeah, you know, I feel like the California State Legislature is not exactly - kind of paper tiger. Not exactly - I'd be more worried about a federal law. But we'll see. I mean...

Steve: Yeah. And I think we're probably going to get one.

Leo: I think what would happen is Apple would appeal it, would tie it up in the courts. You know, it's not going to - it's probably illegal.

Steve: And again, it could end up getting tied into First Amendment rights.

Leo: Well, and CALEA specifically says that the government cannot compel manufacturers of telecommunications devices to do that. So I don't know.

Steve: Right.

Leo: I think this is probably nothing to worry about, but they'll keep trying.

Steve: Yup. So Matt Green, our Johns Hopkins cryptographer, who of course has been very interested in TrueCrypt throughout its life, he was sort of the honcho of the audit, both phases of the audit. And it's been he whom we have quoted about his feelings about TrueCrypt. And of course we know that the original 7.1a code, which I'm still hosting as an archive on GRC.com, that it passed all of the audits that it's been subjected to so far. He tweeted a link to a really interesting story that I commend all of our listeners to.

In fact, I think I made it a bit.ly link for the show, bit.ly/sn-553. I think if anyone puts bit.ly/sn-553 into their browser, I think that takes them here because I wanted to make it easy for people to find this article. It is really interesting.

What Matthew Green tweeted was: "TrueCrypt was originally written by a multimillionaire international arms dealer named Paul Le Roux." And I'm not familiar with this site. It's Mastermind.Atavist.com.

Leo: This actually looks pretty good. This is Atavist magazine. It looks like a really interesting story.

Steve: Oh, Leo.

Leo: Although it reminds me a little bit of the uncovering of Satoshi Nakamoto by Newsweek. You know, I don't know.

Steve: Well, except that...

Leo: Trust Green, for sure.

Steve: I trust Green. And what I wrote in my own notes here is that it comports perfectly with every little scrap of tidbit facts that we do have about TrueCrypt. I remember ScramDisk and, like, its early origins. I grabbed two paragraphs from this. Oh, also, after that tweet, Matthew tweeted: "Paul Le Roux wrote E4M, which TrueCrypt was based on. It's unclear if he funded TrueCrypt itself. He was arrested in 2012 or '13." And then his next tweet said: "Coincidentally, TrueCrypt development ceased around the same time Le Roux was arrested."

So from that story I grabbed two paragraphs. The first is: "Confident in the connection between the two Le Rouxs, I [says the reporter] burrowed into the world of encryption. Le Roux, it seemed, had started building E4M - [which is] Encryption for the Masses - in 1997. It followed that a talented young man so absorbed with the challenges of code, one who had gotten himself into trouble with law enforcement in the past, would tackle a problem as technically knotty as digital privacy." And we should mention that earlier in the story we learned that he'd been coding since high school. He immediately developed an affinity for computers and coding, and that's all he ever did, becoming moderately antisocial and getting in trouble with the law early on, too.

The story, the little bit that I snipped out, continues: "Le Roux's software allowed users to encrypt their entire hard drives and to conceal the existence of encrypted files so that prying eyes wouldn't even know they were there. After two years of development, he released it to the world with a post to the alt.security.scramdisk board. According to his own account, the software was written from scratch, and 'thousands of hours went into its development and testing.'

"In 2004, a group of anonymous developers did exactly what Hafner had feared." There's a reference here that we don't have a context to. Hafner was the president of a company that was commercializing a full-disk encryption product that was based on some of the TrueCrypt work and was open source. And so what Hafner had feared: "They released a new and powerful, free encryption program called TrueCrypt, built on the code for E4M. TrueCrypt is based on, and might be considered a sequel to, E4M, a release announcement stated. The program combined security and convenience, giving users the ability to strongly encrypt files or entire disk drives while continuing to work with those files as they would a regular file on their computer."

So again, it's from Matt Green, stating as a fact that this is where it came from. And if you read through this, I mean, it holds together well. And all of those little bits around the middle of the story, about ScramDisk and DriveCrypt and that company that's mentioned and Hafner, I mean, all of that I remember myself from my own experience at the time.

Leo: I wonder if Green changed his point of view, though, because he's quoted in the story as saying he doesn't know. He says it could have been Paul Le Roux writing under an assumed name, or it could have been someone completely different.

Steve: Oh, you mean Matthew is quoted in the story.

Leo: Yeah.

Steve: Oh, okay.

Leo: So I wonder if he changed his point of view. I mean, does his tweet say, oh, it must have been him? Or, I mean, it's really - it's a great story. It'll probably be a movie at some point. But in the story they quote him as saying we just, we won't, we couldn't, we can't know.

Steve: Yeah, that's odd because his tweet reads exactly this: "TrueCrypt was originally written by a multimillionaire international arms dealer named Paul Le Roux." So he tweeted it as...

Leo: Maybe he changed his mind.

Steve: ...a fact, yeah. So, you know, a little more interesting information. I heard you referring someone over the weekend to VeraCrypt; and I agree, that is the one that people should go to. People are still asking, you know, should we use TrueCrypt, or should we use, you know, or what? And I don't think VeraCrypt yet supports the GPT and the EFI-style booting. I don't think anything does yet. For what it's worth, I'm planning to just use BitLocker because - on my Win7 laptop because all I want is protection against the probability or the possibility that my laptop gets out of my control. And I just want it - I want it well encrypted. And I just want it to work.

Leo: So what I told that person is maybe they could use the built-in ATA lock, the hard drive lock in the BIOS. Is that effective?

Steve: It is very effective, but it can...

Leo: Yeah, I seem to remember you saying that.

Steve: But it can be bypassed by, like, law enforcement.

Leo: Okay. All right.

Steve: Because it contains the key, which is unlocked with a password.

Leo: Got it.

Steve: So it'll beat any bad guys, but there have been instances where those drives have been given to drive manufacturers, and they've unlocked them for law enforcement.

Leo: Probably as good as BitLocker. You know, the other day I installed Ubuntu on a machine, and it has full-disk encryption, which you can turn as part of the install, and you can't get into the disk without entering a password. This is, I believe, it's on a GPT device. It's on my Dell. And then it also has, which I love, additional encryption of the home folder, which might be, for some people, that might be sufficient. Although there would be leakage with the swap files and stuff. But that's built into Linux. We've got to get you off this Windows crap. I just don't understand why you continue to use this. I know because of, you know, your SpinRite and everything.

Steve: Well, I'm still a developer.

Leo: But you don't develop SpinRite in Windows, do you? It's a DOS program. You're using MASM.

Steve: But MASM runs on Windows.

Leo: Oh, you're using Brief and MASM in Windows.

Steve: Yeah, well, MASM is a Windows assembler.

Leo: Oh, okay.

Steve: So, I mean, it runs on DOS, but...

Leo: Bet you could find a good assembler on OpenBSD, for instance.

Steve: But all of SpinRite is in MASM.

Leo: Yeah. Get the macros over, and libraries.

Steve: I mean, I would agree. If at some point I'm doing a rewrite, then it's probably time. On the other hand, I just don't have any problem with Windows. I use 7. Well, I use XP right now. I'm not having a problem. I'm, like, the only person not having a problem because I'm staying with an old one that works just fine.

Leo: Of dubious security, but that's okay. I'm sure you'll lock it down. I mean, you don't care. As long as, I mean, it's in your house. As long as somebody's not breaking into your house, you don't really care.

Steve: And there's nothing here. I tweeted that I was at DMV on Friday because I had to renew my license. I ran out of automatic renewals, and the photo there doesn't look anything like me anymore. There's been a lot of changes in the last...

Leo: Did you have hair in the old one?

Steve: Oh, it was black. I had a big black pornstache and, you know, black hair. And I've had people do a double-take because, like, sometimes they'll need to see my ID for something, like renting a car. Oh, in fact, that's what it was the other day because I was renting - I had my car in for service, and so I rented one for the day that the dealer makes available. And the guy, like, looked at the ID, then looked at me again, then looked at the ID again, looked at me. And I guess he thought, wow, that's a lot of change.

Anyway, the point is that they wanted my right thumbprint, the DMV. The California DMV wants my right thumbprint. And so I tweeted that it's nice that I'm a lefty, and so that's the thumb that I use to unlock my various devices. And then someone said, "Well, now everybody knows." And it's like, yeah. If anybody wants my phone, I'll unlock it for them. There's nothing there except when Jenny and I are going to rendezvous to see a movie. So my life, there's nothing that I'm worried about needing to protect. But I certainly want to stand up for people who want privacy.

So get this, Leo. Oh, my lord. This is just incredible. We've talked about this CA for a while. It's a well-known certificate authority, StartSSL. And one of the things...

Leo: Oh, yeah. Oh, yeah.

Steve: ...they provided was free certificates that had a one-year expiration. And so it was a little annoying that they were one year, but that kind of like kept bringing you back to them, which I guess must have been their hook because they were hoping maybe you'd buy one for three years rather than use the free one for one year. But widely supported. Now, in the back of my mind I have a feeling that I remember mentioning that they were being maybe deprecated from some root stores because they just weren't - they'd done something that caused them not to be trusted.

But what just was in the news was unbelievable. And that is that the method that they use to prove domain ownership turns out to have been trivial to hack, so much so that until last week, anybody could get a certificate from them for any domain they chose. So, okay. The good news is these guys are probably gone, at least from the free CA standpoint, because Let's Encrypt has taken off, and it gives you, I mean, just solves this problem. But the idea is that a certificate authority needs the person requesting a certificate to prove that they control the domain name that they want a cert for.

And so the typical way that's done is the CA will give you a nonce, a random blob file, with the instructions, put this on the root of the server on your domain and let us know when you have. Then they ask for that file on the root of that domain. And if it's there, it demonstrates you have the ability to put files on a server on that domain, thus presumably control of the domain. The alternative is, and many certificate authorities give you this option, is to send email to one of the standard email addresses - postmaster, hostmaster, or webmaster - at the domain dotcom.

So StartSSL offers that option. If you don't want to put a file on your root, you can select with the web interface which one of those three email addresses - postmaster, hostmaster, or webmaster - at fill-in-the-blank domain dotcom you want to receive email. And your reception of email at one of those well-known addresses at that domain, again, is supposed to be proof of domain ownership.

It's even hard for me to say this, it's so unbelievable. The web form that they use sends the email address which the user has chosen as a parameter when you submit it. Which means you can ask for a certificate for www.google.com. Now, they're a bad example because they've pinned all their certificates, and alarm bells go off all over the world if you actually do use a fraudulent Google certificate. But somebody else's certificate, www.ibm.com. And so you fill that in. And when you are given the web form to validate ownership, it will have - you choose postmaster@ibm.com, hostmaster@ibm.com, or webmaster@ibm.com.

But the email address it's going to send the validation to is actually in the form and is sent as a parameter. Which means you can simply change it to Hotmail.com so the verification of the ownership of IBM.com comes to your hotmail address, and you go, oh, thank you very much, click the link to prove ownership. And then StartSSL, this "certificate authority," in quotes, which is trusted by all major browsers, at least until recently - maybe even now, I'm not sure - sends you a certificate, a happy www.ibm.com certificate. Unbelievable.

And as I'm looking at this, I'm just thinking, okay, you know, we have a fundamentally broken public key infrastructure in the industry at the moment. The idea that there is no certification, no validation, no verification of the methodology that these hundreds of equally trusted certificate authorities have in the world is mindboggling. And our browsers trust them all. Wow.

Leo: Wow is right. So, wow. Wow.

Steve: So it was just a free fraudulent certificate mint that you could cause these guys to issue a certificate for any domain you wanted, just by jiggling the web form that they sent you so that it sent back an email with a different domain than they preloaded in the web page that you were then choosing which email address to send to. You couldn't choose the @domain.com. You could just choose the prefix account name. Except that it was all then sent back to the server and accepted, and so you could change that if you edited the HTML of the page they sent. So it was just trivial to bypass that, quote, "protection," unquote. Amazing.

So last week we have another hospital hit with ransomware. This one is called "Locky," which I hadn't heard before, L-O-C-K-Y. So this is a month after our coverage four weeks ago of the Hollywood Presbyterian Medical Center in L.A., which was crippled by crypto ransomware. And that was the - I'm drawing a blank. I didn't write it down. That was the one we've seen often that malicious adware has been dropping on people's machines. So now we have - I'm taking this out of order.

So now we have, sorry, a Methodist Hospital in Henderson, Kentucky initiated what they called an internal state of emergency and shut down its desktop computers and web-based systems in their effort to fight the spread of this Locky crypto ransomware after discovering an infection of its network. The hospital's IT staff posted a scrolling message at the top of the Methodist Hospital's website announcing that, quote, "Methodist Hospital is currently working in an internal state of emergency due to a computer virus that has limited our use of electronic web-based services. We are currently working to resolve this issue. Until then we will have limited access to web-based services and electronic communications."

The Methodist Hospital's information systems director told Brian Krebs, who was reporting on this, that the Locky malware, which came in as an attachment to a spam email, attempted to spread across the network after it had infected the computer it was triggered on. Locky has been known to use malicious scripts in Microsoft Office documents as a means of infecting victims' computers. The malware succeeded in infecting several other systems, prompting the hospital staff to shut down all the hospital's computers. Each PC is then being brought back online individually after being scanned for telltale signs of Locky while it's off the network.

Now, the good news of the story is that, for reasons that are not clear, maybe it's just sort of generic, the Locky guys only want four bitcoins in payment, which is about $1,600, which I consider a massive bargain. I mean, these guys are spending that per hour on IT, you know, emergency recovery procedures. And, for example, four weeks ago, after being down for 10 days, Hollywood Presbyterian had to pay a ransom of 40 bitcoin, which was about $17,000. And even that, you know, when you consider, I mean, I'm sure you know, Leo, all medicine is automated now. I mean, a hospital can't function without its IT infrastructure. And in fact they're literally reduced to writing on, like, stone tablets with chisels. It's just amazing.

Now, that was last week. Yesterday - there is a huge health system in Washington named MedStar Health, which operates 10 hospitals, more than 250 outpatient facilities throughout the Washington region, and has revenues of $5 billion annually. Hit with crypto ransomware. They have no access to their systems. The hospital staff in the reporting on this said they've had to revert to seldom-used paper charts and records. One employee who asked that her name not be used because she was not authorized to speak of the incident said, "Even the lowest level staff can't communicate with anyone. You can't schedule patients. You can't access records. You can't do anything." So they're completely crippled.

And, I mean, I don't mean to be taking this lightly. And it's not, I mean, it's a huge problem. And of course we predicted this years ago. The first time the concept of encrypting a drive and asking for payment appeared on this podcast, we said, oh, this is going to turn out really bad because suddenly there was a profit motive for these kinds of attacks. Until now, I mean, until then, viruses sort of existed just for their own sake, to propagate and roam around. And, well, and there were trojans that were taking over computers in order to commandeer their bandwidth for participation in DDoS attacks. And we see that still.

But now there's, I mean, this is a new deal, the idea that you could encrypt the network of a hospital and get $17,000 of payday out of them, that puts it into a different league. And these people have, you know, we could say yes, back up, back up, back up. It is challenging to keep a real-time backup of something as inherently dynamic as medical records and scheduling and patient history. I mean, the whole infrastructure of a statewide medical system is changing from instant to instant. So, I mean, yes, you certainly do need to have backups. But even that you wonder how current they would be because hopefully - I'm sure that any kind of certification these days requires some sorts of clear infrastructure guidelines. Yet it's also clear that someone clicking on a random piece of email can still bring the whole thing down.

Leo: Whew.

Steve: Wow. So today is Tuesday, March 29th. Two weeks from today will be Tuesday, April 12th. There's been a preannouncement of a major problem with Samba, named after SMB, the Server Message Blocks protocol. Server Message Blocks is the Windows network file system, and Samba is a client and server system written to be compatible with SMB, that runs over on the Unix and Linux family of OSes. I run a Samba server on my FreeBSD Unix machine at Level 3, which is where the newsgroups and my DNS server are. And then I have IP-filtering restricted access to it from my network at home, which allows me to, from my Windows environment, to bring up the Unix system in a very convenient fashion. And so this is the way that Unix environment systems are able to connect to Windows-based systems.

So here's what we know. The site that is tracking this, that has announced this, is called Badlock.org, and so this is called the Badlock vulnerability, B-A-D-L-O-C-K dot org. No one knows what it is, except Microsoft is apparently frantically working on it, as are any commercial providers of Samba and SMB clients and server systems, and the Samba project themselves. They say it is a crucial security bug in Windows and Samba, which will be disclosed.

They write: "We call it Badlock. Engineers at Microsoft and the Samba team are working together to get this problem fixed. Patches will be released on April 12th." That's two weeks from today. "Admins and all of you," they write, "responsible for Windows or Samba server infrastructure, mark the date. Please get yourself ready to patch all systems on this day. We are pretty sure that there will be exploits soon after we publish all relevant information. Patches will be available for Samba 4.2, 4.3, and 4.4," which is the current one.

They do a little Q&A at the end of this, and they ask themselves: "Why announce Badlock before April 12th, 2016?" And they respond: "The main goal of this announcement is to give a heads-up and to get you ready to patch all systems as fast as possible and have sysadmin resources available on the day the patch will be released. Vendors and distributors of Samba are being informed before a security fix is released in any case. This is part of any Samba security release process."

They wrote: "Weighting to the respective interests of advanced warning and utmost secrecy, we chose to warn you beforehand so that everyone has a chance to be ready to install the fixes as soon as they're available. Once the patch is released to the public, it will point to attack vectors, and exploits will be in the wild in no time." And then they ask who found the Badlock bug: "Badlock was discovered by a member of the international Samba Core Team working at SerNet on Samba. He reported the bug to Microsoft and has been working closely with them to fix the problem."

So that's all we know. Now, the name "Badlock" is interesting because of course locking is an intrinsic property of file systems that inherently support sharing because a network file system must. The issue is one of simultaneous contention to resources. What normally happens is somebody will obtain a lock on a file which is an exclusive lock, if, for example, if they want write access to it, so that nobody else can get a write lock that would cause them to create desynchronized copies. So this sounds like - and the fact that Microsoft is involved is really interesting, too, because this sounds like it's an SMB problem, that is, that Microsoft is going to be having to do something, rather than it being a Samba implementation problem.

So anyway, this is all we know. We now know, everybody listening to this knows all anybody else knows, which is in two weeks something big is going to happen. Now, it's also interesting that that is, this being the 29th, that means that April 12 is, and this is probably not coincidental, the second Tuesday of April. So that will be Patch Tuesday, Microsoft's Patch Tuesday. And it's almost certain, if Microsoft is involved and has been involved, that that's why this is happening on the second Tuesday of the month, is that there will be a critical security update for Windows released on that day.

Now, the other thing that's interesting is that Samba and the SMB file system is not normally publicly exposed. I'm using it internally. I have no external presence. And as I mentioned, I've established an OpenVPN tunnel between myself and GRC's servers, and that tunnel encrypts and transports Samba. But again, it's not exposed publicly. Nobody - I can't think of a good reason for exposing a Microsoft file system. Maybe there are good reasons. And if so, you definitely want to be paying attention. I mean, if you for some reason have this exposed, I mean, this is why I created ShieldsUP!. It was because exactly this, because this protocol was being exposed. This was the Microsoft NetBIOS protocol, which has evolved over time. There's a version 2 and a version 3 now of Server Message Blocks. It was once known as CIFS, which has now been a deprecated name because it's moved way past that. Or was it CSIF?

Leo: No, CIFS, you're right.

Steve: Yeah, CIFS. Anyway, so that acronym is no longer used and is considered deprecated. But the reason I created ShieldsUP! was people were exposing this NetBIOS protocol over TCP, which is what the Server Message Blocks protocol, which Microsoft uses to this day, was exposing. So anyway, we will certainly be talking about this in two weeks. And this is one second Tuesday of the month that I will be on top of from the beginning, rather than saying, oh, well, if anything important happens, we'll talk about it next week. I think we can assume that something really interesting will be happening in two weeks. And for what it's worth, if anybody is an administrator of Windows networking, again, the only problem I could see that could really be a problem is if there's something publicly exposed. But why would there be? Again. So maybe these guys are overhyping it a little bit. But, boy, they certainly do seem worked up about it. So we'll find out.

Leo: Might be like a VPN roulette. Did you see that?

Steve: Oh, yeah. VPN or VNC?

Leo: I'm sorry, VNC, yeah.

Steve: Right.

Leo: Lots of fun.

Steve: So good news on the IoT front. And we don't have much information about this yet. But there's something coming from the Wi-Fi Alliance. The Wi-Fi Alliance are the guys, they sort of have a mixed track record because they've brought us really bad things like WPS, which everybody should turn off. And they came up with that broken protocol where two eight-digit keys - I guess that was part of WPS. It wasn't the pushbutton version, it was the enter this code. But it turns out that the protocol was broken such that you could guess the first four digits separately from the last eight, or from the last four, so that reduced it to 10,000. And then it turns out that the last digit was a check digit, and so the last four was actually only three, and it made it trivial to crack this thing in no time. So they don't have a great track record in terms of the security design of their protocols. But they're still trying.

And the good news is they're working on something for the Internet of Things devices because, of course, they're the Wi-Fi Alliance, and our IoT stuff is all WiFi. So they're working towards something called - and I'm sure we'll be covering it in the future, this is right up our alley - the Device Provisioning Protocol, DPP. Their little blurb on their site doesn't say much. It says: "With the increase in WiFi-certified devices available, end-users have the ability to add a more diverse set of devices to their WiFi networks, including a growing range of devices that do not have a rich user interface." Or none at all, like an Amazon buy-it button. "Wi-Fi Alliance Device Provisioning Protocol will enhance the user experience with a simple, secure, and consistent method for on- and off-boarding any type of device on a WiFi network."

Leo: [Grumbling]

Steve: Okay. So that's very mysterious. Network World dug into this a little bit further and has a little bit more to say, which is sort of interesting. And I'll just share what they wrote, or a piece of what they wrote, jumping right into the middle of their article. And I have the link for anyone who wants to read more. "Meanwhile, the WLAN should be protected against intruders impersonating IoT sensors, and real sensors infected with malware. This means sensors should follow the same security regime as enterprise smartphones and PCs. Especially where pre-shared keys are used, the sensor's identity should be established so the WLAN knows what it is, where it needs to connect, and the permitted traffic patterns. Identity can be a userID, MAC address, or certificate.

"But hooking each sensor in turn up to a PC, for instance, configuring it with an SSID, credentials, and identity is incredibly time consuming. IoT vendors are applying their creativity to the problem, and we are beginning to see proprietary solutions. But we would prefer vendor-independent standards." And to that I say amen. I mean, that's what we need. We need this problem solved once correctly.

So they continue: "Garage door openers, home thermostats and the like are often configured by making a point-to-point WiFi connection from a smartphone and entering information on the screen. This model is also applicable to enterprise deployments where an employee is able to stand next to each sensor and configure it. But if credentials are entered on the smartphone screen, they are visible to the employee and prone to error.

"The WiFi Alliance is working to improve this method. The Device Provisioning Protocol (DPP) will allow an already authenticated user's smartphone to bring a new device onto the network, similar to a visitor given guest access by a sponsoring employee. The key feature is to maintain security, keeping the new device's unique credentials hidden from the sponsor and encrypted over the air."

So again, we won't know more until we get some details on what the protocol is. But I'm glad, you know, these are the guys to do it. Let's hope they get it right. And then what we could start hopefully to see is IoT devices saying that they support the DPP, the Device Provisioning Protocol, and that would probably be a good thing because it would mean that we would have a unified, at least something that a group of well-meaning people, rather than individual vendors each making up their own solution, would have thought through and hopefully vetted. And we can hope that they're better with security today than they were when they did the WPS mess.

Leo: This time they'll have four eight-bit blocks or something.

Steve: Right.

Leo: Double it up.

Steve: So I created a new piece of freeware. In this morning's Sydney Morning Herald, Adam Turner wrote in his "Digital Life" column. The column starts off: "As Microsoft ramps up efforts to force Windows 10 onto older PCs, Never10 helps you maintain the status quo.

"Lunch with my parents on the weekend turned into an unexpected tech support visit when my Dad started up his computer to discover it had upgraded from Windows 7 to Windows 10 against his wishes. After months of harassment from Microsoft's nagware, I assumed that he'd accidentally clicked Upgrade, despite his vigilance in closing the popup notifications rather than dealing with the Hobson's choice of Upgrade Now or Upgrade Later. After a quick online search, I realized I owed Dad an apology, as there's been a spate of unwanted Windows 10 upgrades recently from people who swear they never authorized it.

"As Microsoft becomes more persistent, Never10 offers an easy way to put the freeze on Windows 10. It's free software for Windows 7 and 8.1 which makes it simple for anyone to tweak the advanced settings on their computer to ward off the upgrade - something I wish I'd installed on my Dad's computer before it was too late."

So in my case, it was my friend, whom I've spoken of fondly on this podcast for many years, Judy. I met Judy in 1984, when I bought my home from her. She's a realtor and was part owner of the house, and I've known her ever since. I'm the executor of her and her husband's estate, in fact. We became friends. She introduced me to my wife, or the woman who became my wife and so on. So we go way back.

And once upon a time - because she was a realtor, she needs the Multiple Listing Services. She used to have what she called her "modem," which was a TI Silent 700 terminal with the rubber suction cups that you stuck the handset of the phone into. And she would type something, some mystical query into it, and it would roll out on thermal paper all of the multiple listings that met some criteria. Of course, over the years, she went to a PC. Then she was using a modem to connect to some dialup service for a while. That was on 95 and 98 that I was keeping her going on. Then the Internet happened, and she at some point moved to Windows 7.

So she contacted me somewhat hysterically last week, middle of the week, and everything had just become a horror. Judy doesn't understand about URLs. She just thinks, and I know I've made you laugh in the past, Leo, talking about her, because she thinks "The Google" is the Internet. I mean, it's her home page. And so she just asks the magic oracle, The Google, she just...

Leo: I want to go to AOL.com.

Steve: She just types, she just enters English phrases into The Google form, and it magically finds things for her.

Leo: That's what I do. It's magic.

Steve: Yeah. And so suddenly the world just, like, her world changed. She didn't know what anything was. Everything, you know, it was a big disaster. So Jenny has safely moved over. I moved her to a Mac, so she's all happy. She loves her Mac. She doesn't know why it took her so long. And so she's no longer in danger. But this was just a cataclysm for Judy. And it turns out that whatever it was that happened, it wouldn't revert. It was supposed to revert, but it didn't revert. So it...

Leo: That's the real problem because you will get the EULA, and you click Yes, and then you're in Windows 10. But if you click No, then it tries to revert. But if it doesn't revert, now you're worse off than ever. They've basically screwed your machine up.

Steve: Yeah. So, okay. So I also, I'd been talking about the GWX Control Panel for a number of months, and it's what I was using on my Win7 machine. But I had sort of started not to like it. It was popping up and announcing itself all the time and talking about what a great job it was doing. And I just wanted it to just be quiet. And then there was something I needed to do, and I looked at it, and it's covered with buttons, and it's got a whole screen full of, like, all of the things it does and what it's doing. And it's like, press this if you want this, and press this if you want that, and press this. And there's, like, 12 of those. And it's like, I just don't want Windows 10. And so I thought, okay.

And, of course, our listeners know that some months ago I also discovered Microsoft's official solution to this. Back in July they updated Windows Update. Probably around the time they were getting ready to add what they call "OS Upgrade Features" to Windows Update, they had the sense of adding some new registry hooks that would disable the Windows, I meant OS Upgrade, sorry, OS Upgrade.

So, and I've talked about it on the podcast. In fact, I created a bit.ly link. It was bit.ly/no-gwx. I talked about it weeks ago. That takes you to the Microsoft Knowledge Base page where you can navigate through which version of Windows you have, and then which sub-edition you have, and then x86 and x64 and so forth. And then the point is that you need that upgrade in order to incorporate these new options. And then the problem is you need to use the Group Policy Editor or edit the registry. And Leo, I've heard you mention on The Tech Guy that, like...

Leo: Don't do that.

Steve: ...there are ways to do this, but, you know...

Leo: Well, I love your approach because one of the concerns, besides all the buttons on GWX, is that he has to keep it up to date because he's fighting a cat-and-mouse game with Microsoft. But Microsoft has always said we'll support your group policy edits, your settings. They're not going to override that because that's how Enterprise works, and that would be the end of the line.

Steve: Right.

Leo: So what you've done is brilliant, actually.

Steve: So for people who don't know - and, boy, I'll tell you, this thing has taken off like a rocket ship.

Leo: I bet.

Steve: If you google "Never10," it's just pages.

Leo: Well, can I just congratulate you on excellent marketing because that name is half the reason you're getting links, I'm telling you, is the name Never10. Yeah. Mainstream media loves that.

Steve: So we're at about 27,000 downloads.

Leo: Yikes.

Steve: And it has immediately jumped to the No. 1 rank of GRC downloads. So all it is, and it annoys me that it is 81K because, get this, 56K of its size is the high-color, high-resolution icon.

Leo: A bitmap. Oh, okay. Well, they're bitmaps, yeah.

Steve: Yeah, yeah. 56K of my 81 is just icons.

Leo: The code is just a few K, yeah.

Steve: Well, and the signature, I have to have a cryptographic signature. That adds 4K. So it would be 21K if I didn't have to carry all this ridiculous goofy baggage around.

Leo: Steve, 21K, all you're doing is modifying the GPE. Really? You could probably do it in 4K.

Steve: Well, except it has a nice UI.

Leo: Oh, a UI, oh.

Steve: It's got nice color screens. You can see what your status is. So here's what it is. It's super lightweight. It does not install.

Leo: I love that, too.

Steve: If you run it on something that cannot have the OS Upgrade, which would be an Enterprise edition of 7 or 8 or 8.1, it tells you that you're using an Enterprise system, so don't worry about it. Or if you try to run it on XP or on Windows 10, neither of those, you know, 10 already has the curse, so there's no point in telling you that it's too late. Or XP of course isn't a candidate. So it just tells you it's only for 7 or 8.1. Then it checks the current version of the Windows Update client, which is one of the things, it's in the Windows systems directory. It looks at the version number, which is different for 7 or 8.1, to make sure that you've got the version number which supports these features, these new registry keys. If not, then it tells you that you need to update your version of Windows Update, which it'll do for you. You just press a button. It goes out and pulls one of four files from Microsoft's Windows Update server for 7 or 8.1.

Leo: I apologize. This is more complicated than I thought. There's a lot going on here.

Steve: Yeah. But the beauty is it's all hidden from the user. The user sees none of this. So it pulls one of four files and runs the standalone installer to install Windows Update. So then the screen comes back and says, okay. Now you're - oh, and then, since it assumes the only reason you're doing this is to disable it, it then also sets the keys for disable.

Now, the other thing I did, I went one step further. First of all, I verified that the group policy edit, all it does is set the registry key, which means we don't need to mess with group policy. This is all in the registry. So there are two keys that it sets, or two values under keys. After it sets them both to disable this behavior, it then edits the privileges on them. The way the registry works is it's a hierarchy of keys, in the same way that a file system is a hierarchy of folders that end up containing files. In a file system, the access privileges are typically inherited from the parent. And that's the same as with the registry. So these keys inherit their privileges from their parents, which typically inherit the privileges from their parents.

Well, I terminate the inheritance of the privileges on these keys and then assign read-only access to everyone. So all system processes, including Windows itself, are able to read the keys. Nobody can change them. And then, if you use Never10 again - because you can flip it back and forth as much as you want. If you later decide you want to reenable this, it removes the privilege block, allowing the normal privileges to flow back down into the keys. And then it deletes both values, as if it had never existed. In no case is anything installed. So you can run it once, set your system the way you want it, and then delete it; or, you know, it's 81K, you can leave it around.

Now, the other thing that I was very impressed by is that, in all of my testing I did over the weekend, even if Windows has already downloaded its at least 3GB of getting ready to upgrade you to Windows X files, if you subsequently use this approach to disable Windows Upgrade, Windows' own GWX tools delete that 3GB. And so I don't have to do it. So that was, when I saw that, it was like, yes.

Leo: Even better, yeah, yeah.

Steve: I was very impressed. So one of the...

Leo: Download 81K and save 3GB.

Steve: Right. Well, and one of the problems that the GWX Control Panel guy has is he's trying to keep GWX off of your computer. Well, it's tiny. You can go visit it. It's in the Windows\System32\GWX directory. It's about 30MB, which it's not nothing, but it's not big compared to anything else. And the point is that the presence of these keys completely hold it at bay. People make the mistake of trying not to install - 3035583 is the update. And so they keep trying to, like, they uninstall that, and then they hide it. And the problem is every month Microsoft unhides it.

And again, I looked a lot at the whole Windows Update system and whether I wanted to get involved with that as part of this. And it is just a mess. There's no way to firmly prevent Windows updates from loading. They don't provide the facility. They have sort of this soft hiding thing which hides it from the UI, which will prevent it from installing. But Microsoft on a whim can choose to change that. And in fact, when they update their updates, these things reappear again. And of course...

Leo: This was actually part of the deal with the free upgrade was that you had to agree to updates. You can defer them, but you cannot refuse them.

Steve: Right. Right.

Leo: So that's, I mean, they were explicit about that. It was in a EULA, but they also were very clear about that, that that was going to be the quid pro quo.

Steve: Right. And so anyway, I like this approach. This doesn't prevent anything from happening. It lets Microsoft do its work. But it is, in all of the testing, not only does it prevent it from ever offering this stuff to you; but, even if it's already there and staged and ready to go, it removes it itself when it sees you don't want it.

Leo: Good.

Steve: So I think this is a complete solution for the problem. It's tiny, lightweight, and just does the job.

Leo: Fantastic. Well done. Bravo.

Steve: Thank you. I did find some people whose Authenticode system was complaining about my SHA-1 cert, which didn't expire until July. So I only discovered that yesterday. And once again, DigiCert came to the rescue. In a matter of minutes, actually, I was able to get from them an SHA-256 Authenticode signing certificate. Now, the problem with that is that Microsoft's SmartScreen hasn't seen software signed by it before because it was freshly minted. So some people who are installing it, and I put a note to that effect on the download page for Never10, they'll see SmartScreen saying, oh, we don't know what this software is. It's like, yeah, yeah. You just click on More Info and then run anyway, and it'll - and I guess it takes a few days for Microsoft to decide this is, you know, things signed with this new certificate are fine. So this is the certificate I'll be using from now on.

So I did want to mention I was looking at GRC's download page. This has replaced the DNS Benchmark, which I wrote I don't know how many years, but it was like 2,000 days ago because my little counter there shows days since the file has changed.

Leo: It's like six years. That's great.

Steve: 2.53 million downloads of the DNS Benchmark. SecurAble is older and has 3.675 million downloads. And what's weird about that is that it's not for the functionality I designed it for. It became super popular as the way people could find out whether they had 64-bit-capable chips in their machine. Because as a side effect of what SecurAble does, I show whether you have a 32-bit or a 64-bit chip. And so when we were in this early stages of Microsoft offering 64-bit versions of their operating systems, or even in some cases people wanting to move to 64-bit non-Windows OS, they didn't know if they had a 64-bit capable chip because they just didn't know what the history of their machine was. So SecurAble was being downloaded, was being recommended by lots of other sites saying, hey, do you want to find out if you can to this with 64 bits? Go get this little SecurAble thing from GRC. It's super tiny, and it just - it'll tell you. So 3.675 million downloads later.

Unplug n' Pray blessedly is slowing down, only 377 downloads a day of that now. But it's nearly 4 million downloads. And the all-time record-breaker is LeakTest at nearly 8 million downloads of that little venerable tool, which people will remember I created to see whether outbound blocking was available in their firewall back in the day. So fun stuff.

Leo: Nice.

Steve: And anyway, new piece of freeware, Never10.

Leo: At GRC.com. Look in the software section.

Steve: So, Leo, toward the end of your podcast, The Tech Guy podcast on Sunday, you had a guy who was wondering about the bandwidth of his, like, his whole home's bandwidth usage.

Leo: Yeah, he wanted to know by application.

Steve: And so I wanted just to note that one thing I wasn't aware of until I stumbled on it, and I think it might have been actually another user of it who told me, is that freeware that I had mentioned called NetWorx, N-E-T-W-O-R-X, it offers a one-button configuration to monitor the SNMP broadcast or service on routers. SNMP, I don't think we've ever talked about it. It stands for Simple Network Management Protocol. And it is a well-standardized protocol, Internet protocol that allows devices or clients to query the configuration or current status of network-connected devices.

And so, for example, many devices, all of the devices I have, like higher-end devices, all support SNMP. It's an option that you can install even in Windows and make your Windows device SNMP queryable. So, and it uses this weird OID naming convention where it's really, really long strings of decimal digits, you know, 3.1.2.7.6.5.4., you know, 7.22, you know, it's just, like, crazy. Nobody memorizes them. You just use a dictionary to look them up. But they're universally standardized, so much so that it's possible for an SNMP client, which NetWorx is, to know how, without any configuration, to know how to ask your router, your main border router, for the number of packets or bytes, yeah, bytes, sorry, the number of bytes it has sent and received on its WAN interface.

So, and that's the way I've configured my copy of NetWorx, no longer monitoring my own system's interface. I have it instead querying through SNMP the WAN interface on my main border router, so I'm able to look at the instantaneous incoming and outgoing traffic on the entire network. But then NetWorx goes a step further because it has a ton of bandwidth management features, where it's able to accrue this over time and with, like, monthly usage and daily usage and hourly and break it down and give you all kinds of controls.

So I just wanted to let - the question on the weekend prompted me to remember that I had not ever mentioned this on the podcast. And I wanted everyone to know because it's just, it's really cool the way it works. It just, you know, you press a button, and suddenly you're looking at your router's WAN interface, no matter what router you have, because they publish SNMP on the LAN side.

Leo: Nice. That's really great, yeah. You forget your login, you can always do that.

Steve: Yeah. And just this is so random, but the Temperfect Mugs are reportedly weeks away.

Leo: Yeah, yeah, yeah, yeah, sure.

Steve: And I'll tell you, Leo, this whole crowd-funded thing is such a mixed blessing.

Leo: Have we learned our lesson?

Steve: Yeah. I am glad, though...

Leo: You know, on the other hand, there are some good things. Go ahead.

Steve: Yeah. I was going to say I'm glad that, at the time, back then, what was it, three years ago or something, I bit the bullet and bought, like, the $300 Darth Vader black special coating thingamajig because to read these guys' postings, they are amped. They are so happy with - I know. I know. We'll see.

Leo: Have you learned nothing?

Steve: Oh, no. I'm the eternal optimist.

Leo: But let me tell you a happy story because I did kick in on the Oculus Rift when it was a Kickstarter. And I got the dev edition. And, you know, it was funky. I think I gave it to Chris, our intern, a year or two ago. He was really excited about it. I doubt he's even doing anything with it. And then they got bought by Facebook for billions of dollars, and I thought, well, so much for that. I'm glad they used my money wisely. But I was so gratified that they are sending, in fact, I just got an email, it's going to come this week, sending me the release version, and everybody who kicked in on Kickstarter. They have no obligation to do so. It's probably at significant cost to them. But all of the people who supported Oculus early on are going to get, before anybody else, I think, going to get a Rift.

Steve: Nice.

Leo: So I think that's, yeah, so there are some happy stories. Whether I'll ever see my floating bonsai tree is another matter, but...

Steve: I did get the Neuroon, N-E-U-R-O-O-N, I think it is. It's a sleep mask that also does EEG. And it's got LEDs that are supposed to, like, wake you up at the right time. And it's like, okay, well, I haven't - I've had it for a few weeks, and I haven't bothered yet because I'm so happy with the Zeo.

Leo: Right.

Steve: Which I'm using, and I know how to read it.

Leo: That's the big problem is sometimes these things take so much longer. Like I ordered, like, a $100 modular smartphone case called the NexPaq. And I'm going to get it, I think, in the next few months. But the problem is I ordered it two years ago. It's going to be for a phone I haven't used in a year and a half. And it won't fit anything I've got. But I'll have it.

Steve: Yeah. I mean, clearly the takeaway is that well-meaning amateurs who are creating ambitious products, they may succeed; they may fail. We hope that it works out. But, boy, it normally takes a lot longer than, well, I mean...

Leo: It's hard.

Steve: That's the experience with any big complex project is that these things take longer than one expects.

Leo: Right. It's hard.

Steve: Okay. So anybody listening who is not interested in the machine I built can...

Leo: Tune out now? Okay, everybody's leaving. Go ahead, get out of here. Goodbye.

Steve: You've had an hour. You've got all the news of the week.

Leo: They're all leaving. They're like rats deserting a sinking PC.

Steve: That's fine. I don't want to bore anybody...

Leo: Man.

Steve: ...with the details of the box I built.

Leo: No, I'm really interested. You know, we're building one, too.

Steve: I know.

Leo: We're building it for the Oculus Rift. But I have a feeling we're probably doing something fairly similar.

Steve: Well, there are some differences because I've heard you mention liquid cooling.

Leo: Yeah.

Steve: And I went with air cooling. So anyway, just to finish that, anybody who's not interested, it's the end of the podcast. You've got all the news for the week. You're warned about the sky falling two weeks from now with Samba. We'll be on top of the second Tuesday. We'll probably do a Q&A next week, so please feel free to hit stop. And we'll pause now for a minute for you to do that.

Leo: [Humming] Okay. Is everybody gone?

Steve: All right.

Leo: Okay. Now we can talk. Nobody [crosstalk].

Steve: All right. They've all left now. So now we just have the people who care.

Leo: Everybody cares. Go ahead.

Steve: So as I mentioned at the top of the show, my goal was to build what I'm calling "My Last PC." It could very well be. I generally build these things - I build them infrequently. And when I do, because I don't want to spend time building them every year or two, I build them to last. And I build them, not only to last in terms of endurance, but I go to the top end as I am able at the time so that when I start using it, I'm off to a good start. And however much RAM...

Leo: You're future - that's called future-proofing.

Steve: Yes, exactly, thank you. Exactly that. So that was the goal with this. I have had very good luck with Silverstone cases. Those are the ones, Silverstone specializes in home theater PC cases. So they're large, easy to work with. They have both pedestal and desktop. I wanted a desktop case because I wanted to get it up off the ground. The ground tends to be a little dusty down there, and I like having it up on my desk. The other thing these cases are is extremely quiet. And also lots of ventilation.

So some of my criteria were I wanted it to be desktop. I wanted lots of large fan ability on the case and for it to absolutely run quietly so that I literally couldn't tell that it was on. I've never messed with water cooling, so I just thought, you know what, that's a bridge I don't want to cross. So I went with a high-capacity large tower cooler that would fit in the case. And in fact the first picture of the pictures shows the one I...

Leo: This looks like an engine block from a '56 Chevy, is what this looks like. This is like a radiator from a truck.

Steve: Yeah. Now, that shows the one fan with the radiators on both sides. And this is a company - I don't see their name anywhere. Noctua, N-O-C-T-U-A, dot A-T [Noctua.at]. Yeah, Noctua. And these guys make fabulous cooling stuff. Now, the way I set it up, as we will see in a later picture, is actually, and they provide the clips for it, is another fan on the inside of the inner radiator. So it's essentially sort of the middle fan is a push-me-pull-you. It's sucking air through the outboard radiator and then pushing it through the inboard. But I thought, oh, well, if one fan is good, two is better. So I mounted another fan on the inside radiator to give a little more pull.

Now, the next picture on the show notes is the inside of the case looking into it. I ended up replacing those two large fans that you can see at the top of the picture with Noctua fans. I went completely Noctua throughout after doing some research. They're all hydrodynamic bearings, super quiet, super long life. Basically there's no - it is a dynamic fluid bearing that is closed and just will go forever.

So this case features, basically one whole side of it is two 120mm fans. You can see down at the bottom an 80mm, actually I think it's a 95mm fan opening at the bottom. And the concept is that air moves, in this picture, from the top to the bottom. And because the front on this picture is facing to the right, it's moving from the right to the left. But so I'm very conscious of air moving through the case, in one side and out the other. And there's another pair of 80mm fan openings above the whole I/O port region. Also notice that the RAM sockets are aligned with the air flow also, so that the air will be flowing through and along with the orientation of the RAM, not fighting against it, which is also important.

So in the next picture we can see I've mounted the two 3TB hard drives. Those are mounted to the inside of the front panel of the case. And I used, again, because I want to keep them cool, I had really good experience back when I was using large drives in my expanded TiVo Series Ones. I mounted heat sinks on the drives and then fans on top of the heat sinks. And I was amazed how much cooler they kept the drives. So in this case what I've done, since I have airflow, now that the case has been switched around in this photo so the air is flowing up the screen from those two - and you can see that I've switched all to Noctua fans, so there's the two big 120mm fans on the bottom.

Now the heat sink, the processor and the heat sink are mounted, so you can see the heat sink for the processor is right in front of the fans taking the external air which is being brought in from those two fans, propelling that air through the two big radiators into the inside. And then the air is being pulled out, actively pulled out, by the smaller fan, the 95mm fan up at the top. And that's deliberately turned around to make sure that it's pushing air out, rather than pulling it in. And also the two fans over the I/O area, the two 80mm fans, those are arranged also backwards, so they're pushing air out the back of the case rather than pulling it in. So the only air coming in are the two largest 120mm fans. All the other fans are pushing it out, and the heat sink, the processor heat sink is right there taking the incoming cool air and pushing it through.

Leo: I'm a little worried, though. You have a lot - you're going to have some turbulence in there because you don't have a straight-through flow. You've got fans sucking here and here and pushing there and there.

Steve: Yeah.

Leo: Before you turn this on, you're going to have to blow some cigarette smoke in there and see what happens. I'm not kidding. Because you can actually have too many fans, as you - I'm not telling you. You know this.

Steve: Yup.

Leo: And you really want to make sure you have - you may not need as many fans as long as you have a good consistent free flow.

Steve: Correct.

Leo: Blow a little smoke in there, some incense, you know, whatever.

Steve: It is, because of the coming in the bottom, going out the top, that the heat sinks, what I used for the hard drives is I used the same heat sinks that I had once used, just big beautiful massive copper heat sinks, where the fins of the heat...

Leo: They're beautiful, yeah.

Steve: Yeah, the fins of the heat sink are aligned with the air flow, the in from the bottom, out through the top. And I used a thermally conductive epoxy. It's like $5 on Amazon. So it's actually epoxy, a two-part compound you mix and then smear around and sets in about five minutes. And so they're just on there forever. So those are the two 3TB drives that are mirrored, which are sort of the master image backup of the system.

Leo: That's funny. That's exactly what we're doing. And I presume you have an SSD in there, as well.

Steve: Well, I was just going say, look there, it's right there in the picture. You can see it sitting right in the middle of the four silvered sockets.

Leo: Oh, yes, there it is.

Steve: It's a Samsung.

Leo: And the same one we bought, yeah.

Steve: Yup, the Samsung 920. And so that...

Leo: 950.

Steve: Yeah, right, 950, which is a 512GB...

Leo: Great minds. That's exactly what we got.

Steve: ...SSD.

Leo: Yup.

Steve: Yup. And so it's in the M.2 socket, so it's right on - so it's a PCIe interface. It is blazingly fast.

Leo: Oh, yeah.

Steve: And so it has a direct serial bus to the processor. And then, if we go down to the next picture, we can see the one other thing that I wanted, and that was a graphics I/O. I didn't mention that the board I chose...

Leo: You're playing videogames? Now, this you've gone way beyond. You're doing SLI. We're not doing that.

Steve: Well, no, I'm actually not.

Leo: Oh, it's not two cards? Looks like two cards.

Steve: Well, yeah, there are two cards.

Leo: Oh.

Steve: But they're not SLI. They are each quad HDMI.

Leo: Oh, you've got Quadros in there. Oh, I get it, okay.

Steve: Yes, exactly. Because, for example...

Leo: That's more for graphics design than gaming.

Steve: Well, actually it's the way I roll. Like right now, Leo, I've got a screen in front of me when I look down which is my main working screen. Up here is normally TweetDeck, but it's also a second instance of Firefox with a bunch of tabs. I've got Firefox always open here as my portal to the world. This screen up here is monitoring the server with charts showing everything that's going on at GRC. Over here we sort of have a scratch screen where Explorer is open in order to allow me to move files around.

Leo: So you're going to have four monitors, is what you're telling me.

Steve: Well, I have five here, and this system will drive eight.

Leo: Eight monitors.

Steve: Yeah. And then the only other thing is you can see that I ran eSATA out to a clip on the back. I also ran a bunch of USB 2.0 and two ports of USB 3.0 out the back. So other than that, I mean, and that is it, finished and working.

Leo: Looks good.

Steve: Yeah. And so...

Leo: Yeah, looks really good.

Steve: And so I did mention...

Leo: People don't pay enough attention to the heat from the hard drives. I think it's really smart to put radiators on the hard drives.

Steve: And it's amazing what a difference it makes. That's the point I wanted to make was just giving them a chance to shed their heat makes an incredible - it just, like, drops the temperature 20 degrees. It's like, in fact, sometimes the drives are, like, when I had a fan on the heat sink, I don't here, but the drive was actually cold because the fan was pulling heat out aggressively through the heat sink. So this is just a passive radiation of heat from the drives. But it'll just keep them running cooler.

Leo: How noisy is this thing?

Steve: This thing will never go - I never turn this...

Leo: It's not noisy?

Steve: No. It makes no sound at all.

Leo: Oh, interesting.

Steve: It's absolutely quiet.

Leo: That's - they're big old fans, so that keeps them quiet.

Steve: And then the last page is a picture of the BIOS screen, showing it running, where the processor - so there are eight cores because it is an Octa-Core. It's an 8-Core I7 with the largest cache that they had that Intel made. I think the chip was $1,200 or something.

Leo: Wow. Holy [crosstalk].

Steve: And you can see that I'm clocking them all at 4.3 GHz.

Leo: You got the K's, the K variety, which is unlocked, so you can do that.

Steve: Yeah. So it's unlocked. And so the reason I'm a little uncomfortable with the motherboard...

Leo: Geez, Louise.

Steve: Yeah, so...

Leo: So funny.

Steve: Yeah, so...

Leo: Why are you uncomfortable with the motherboard?

Steve: Well, because I would like to be able to drive 128GB of RAM at 3200 MHz. And what you can see in this picture is every other slot is occupied - 1, 3, 5, and 7. They each have 16GB. So I have a total of - and I'm not saying "only," but, well, half of what the motherboard could hold of 64GB...

Leo: I think 64 is enough.

Steve: I think it is.

Leo: I don't think you're really running, I mean, what are you going to run on this thing?

Steve: Well, see, I want to make this a happy place for virtual machines to run.

Leo: Ah, okay.

Steve: And VMs take up a lot of space.

Leo: Right, okay.

Steve: You know, each VM wants to have its own 4GB to play around in.

Leo: Right, at least, yeah, yeah.

Steve: Yeah, exactly. So that was my plan. Now, what I found was, if I fully populate the board with 128GB, even though the RAM is 3200 RAM, the capacitive load of the additional chips forces me to bring it down to 2.66 GHz. So I can run 128GB of RAM at 2.66 GHz stably; or 64, run half that much, 64GB at 3.2. So my choice is 64, as you note, is probably plenty. But if I ever need more, I actually, I have the RAM. I'm going to keep it. And I could always add it to the motherboard and then slow the RAM down if 64GB is ever insufficient.

Leo: Smart man.

Steve: So anyway, that's the machine I built.

Leo: I'm thinking you will never buy another computer. I think I agree with you. I can't, I mean, if you did, it will be for - it'll be purpose-built for something like VR. I mean, this, for instance, you couldn't run Oculus Rift on this.

Steve: No.

Leo: Because you chose Quadros.

Steve: Well, yeah.

Leo: I mean, not that you didn't spent a lot on your GPUs, but they're just not, you know.

Steve: The motherboard I bought...

Leo: Is SLI.

Steve: ...is an SLI motherboard. And that's one other, so a lot of people have asked, oh, you know, what motherboard did you choose? The reason I'm unsure about it, and I almost scrapped it and tried another one because...

Leo: We got the ASUS, which I really like.

Steve: And so I don't know if it ought to be able to drive 128GB at 3.2 GHz.

Leo: Oh, I think we have the same thing. I think we're using 2800 RAM for the same reason. I'll have to ask Ryan Shrout. But I think that that's not the motherboard. Maybe it is. You think it's electrical, like it just can't, doesn't have enough voltage to do it, or...

Steve: Well, it's drive. It's the idea is that it's driving four DIMMs at 3.2 GHz. But when I put eight in, it can't do it.

Leo: Right.

Steve: And so I have to slow it down.

Leo: Yeah.

Steve: And so that says that there is a capacitive load, and it just isn't able to, because of the additional capacitance created by the additional memory, the processor just doesn't have the instantaneous current to charge and discharge the wires fast enough.

Leo: We talked about this, and I don't remember it. But if you go back to The New Screen Savers a couple of weeks ago, when Ryan talked, we talked about the memory we put in, that sounds familiar. And I know we're using 2800. So I think that that sounds right. I think he said, if we put more RAM in, we'd have to...

Steve: Slow it down, yeah.

Leo: Slow it down, yeah.

Steve: And the other problem with this motherboard is, because it is an SLI, that is, because it assumes you're going to be putting in a powerful video, it has none of its own. And so most...

Leo: Oh, interesting, yeah.

Steve: Yeah.

Leo: We have motherboard video. I mean, it's like comes with the territory. It's like, they throw it in for free.

Steve: And so, yeah. And so it's like I missed that when I bought the board. It's like, what, no built-in video? It doesn't. It's got none.

Leo: It's meant for doing what you're doing, is what it is.

Steve: Right, right. And in fact I would be using these eight videos. And these are all able to do the big size, 2280 by 1900 or something, so like monster resolution.

Leo: Yeah, yeah.

Steve: Four times...

Leo: Yeah, this is what quad - Quadros aren't the fastest in the world. I mean, they could be.

Steve: Right.

Leo: But they're designed for graphics designers and very high resolution.

Steve: Right.

Leo: I think that's a great choice. For what you do, that's the best choice.

Steve: And again, passively cooled. There's no fan on them. And again, I've designed them so that air flows out through the slots. And there's a slot empty between them so that there is a vent slot adjacent each of the heat sinks in order to allow the air to get out.

Leo: Water cooling has really - nothing wrong with what you're doing. And, you know, obviously. But water cooling has come a long way since I was doing it. And these are sealed units. They go in very easily. They have heat sinks specifically for various parts. It couldn't be easier. It's a lot easier even than when we built our ultimate game machine 10 years ago. Gosh, is it that long.

Steve: And I guess it takes a lot less space, doesn't it.

Leo: Yeah, yeah. I mean, now it's a whole different - the game has changed quite a bit.

Steve: Right.

Leo: I'm interested that you're overclocking, though. And you're not overclocking insignificantly. I mean, those are 3 GHz chips; right?

Steve: Yup.

Leo: And you're running with 4.3 GHz.

Steve: Yup.

Leo: That's a lot.

Steve: Yeah, and they're running cool.

Leo: And it's reliable. Wow.

Steve: Yeah.

Leo: Did you bump the voltage a little bit to do that?

Steve: Yeah. I definitely had to bring the voltage up in order to drive them that fast. But not up to a dangerous level.

Leo: Interesting.

Steve: Yeah. So, but it ended up...

Leo: It just shows you that chip has a lot of headroom.

Steve: Oh, it goes, yes, yes, yes. And I'd spent a lot of time digging around, trying to see if there was any indication that there would be a shortening of the chip's life pushing it higher and hotter, and there isn't. And it is, you know, Intel has all of this stuff set up dynamically. I mean, so one of the things I kind of maybe should have done is, rather than going eight cores, maybe I should have gone to a quad core and gone with - was it a larger cache? It might have been even a higher speed in a quad core.

Leo: Probably, yeah. That's relatively slow, that rated speed.

Steve: Correct, correct. And because the only thing I'm really thinking would be major video compression, like when I'm recompressing something that - and I do that from time to time, and that always takes a long time. So that's something that will pin all 16 - because each of those cores is hyperthreaded. So there's 16 threads. And, boy, when you bring up Task Manager and look at it, it's like, oh, my god. It's like, you know, 16 individual execution threads in this thing. But they'll all get pinned because FFmpeg is now able to run a massively multithreaded...

Leo: Oh, man. You're going to get some great rendering performance out of the thing.

Steve: Yeah.

Leo: That is awesome. Wow. Can I ask you how much?

Steve: I have no idea.

Leo: You've never added it up. Wise man.

Steve: I didn't add it up. I just said I need one of these, I need one of these...

Leo: That's a man who does not have a wife, my friends. No one to answer to, yes. I don't know. It cost what it cost.

Steve: Yeah, I did, I took advantage of NewEgg's and Amazon's nice return policies because I messed around with the RAM for a while. I got some RAM, and then when it didn't go fast enough, I sent it back, and I got some others.

Leo: Perfect.

Steve: So I had at one point three different sets of RAM that I was swapping around, trying to see, like, where the sweet spot was and what could I make it do and so forth. Because it was like, you know, a lot of patchwork. But everybody took everything back that I ended up not keeping because that's part of the bargain.

Leo: You have to really good retailers, I think. They're excellent.

Steve: Yeah.

Leo: Neo in the chatroom is saying that processor, you're not going to run more, you can't run more than 64GB of RAM. He says you'd max it out.

Steve: I do run 128. It works.

Leo: It works. Okay.

Steve: Yeah.

Leo: Okay.

Steve: Yeah, it took it.

Leo: It took it. You just had to slow it down.

Steve: I had to slow it down to 2.66.

Leo: And I think there's no - you're not getting any speed benefit going from 64 to 128GB of RAM, so you might as well run, you know, it's, you know.

Steve: Yeah. Empty RAM is doing nothing.

Leo: They're not doing anything.

Steve: Yes.

Leo: But I do see, if you're going to run - how many VMs are you going to run on this unit?

Steve: Well, I just don't want to not be able to run any, you know.

Leo: Yeah, you could run eight.

Steve: Yeah. Well, so, exactly. And so to be able to, like when I'm working on SQRL, I need to be using Ubuntu because I want to make sure that it runs well under Wine. And so it's just nice to be able to have that open. And I'm probably going to end up with some sort of a browser-in-a-box environment where I move Firefox into its own VM so that any games it wants to play there with malware can't get out. So anyway, so one of the goals was, because I've been feeling the limit of 3GB in my 32-bit system, I just said, okay, I'm going to, again, I want this to be the last thing I build.

Leo: This is not the same exact processor. You used the K, not the X. But 20MB of cache, that's nice. That is really...

Steve: Yeah, it has a lot of cache. And nothing is more important than cache. As we know...

Leo: Oh, yeah.

Steve: ...cache is king. And that's one of the nice reasons why having only a few cores in use normally means that the large cache is designed for sharing. But there won't be sharing very much. Mostly I'll just be able to open...

Leo: Oh, it is the X. I misread your BIOS. It's not the K, it's the X. So this says, on the spec, it says max memory size, depending on memory type, 64GB.

Steve: Huh.

Leo: So send that RAM back.

Steve: Well, you know, what I'll do is I'll just keep it because, I mean, I did have it in, and I ran a memory test because I wanted to verify that it was solid, so I know that it runs 128GB, even though...

Leo: There's something wrong here. This can't be the same processor. I mean, it also says your max RAM is 2133. I don't know. This might be the wrong page.

Steve: Or maybe it's Intel being conservative.

Leo: Well, as they are.

Steve: Yeah.

Leo: As they will be.

Steve: Yeah.

Leo: Nice. What is the monitor? Are you going to use your existing monitors?

Steve: Yeah. I have some nice Dells. I've always liked Dell monitors. And I have, because my current monitors are DVI, it turns out that you could just do a little dongle, which is an HDMI to DVI.

Leo: Yeah.

Steve: And so initially I will just use the little HDMI DVI converters to run the existing set of monitors. And then as I, over time, as I swap these monitors out, the new ones will certainly be HDMI. And so then I'll just remove the little dongle.

Leo: Easy-peasy. Yeah, that's one issue we're going to have because it turns out the Oculus Rift needs the HDMI port. So we're going to have to use, I don't know, we're going to have to use some funky interface for the monitor. But, you know, you don't need a monitor when you're in the VR there.

Steve: Oh, and I did forget to mention the Corsair power supply, the RM850...

Leo: Yes, yeah, I think we got the same one, yeah, very nice.

Steve: Yeah. And that's about 200% the size I need. Based on the calculations I did, it was like around 400 watts maximum. And so I thought, okay, I'm just going to give myself plenty of headroom because you don't want the power supply - in fact, the power supply's fan doesn't even run. And they warn you not to worry if the fan is not turning because it only spins the fan up when it needs to cool itself off.

Leo: Yeah. That's good. So how many watts in the power supply?

Steve: 850.

Leo: Yeah. Yeah.

Steve: And those monsters, you can go all the way up into the 1200s or 1500s.

Leo: Well, that's the nice thing about Corsair, unlike some of the brands. I mean, they really, they live up to their rating.

Steve: And it's modular, so you only plug the wires in that you need.

Leo: Right.

Steve: And, yeah, and most of it's empty.

Leo: That's my job tomorrow. Now that the Oculus is coming, we have to put all the wires in.

Steve: Oh. Well, actually, you got a nice case.

Leo: Oh, I love our case.

Steve: Your case allows you - you're able to run the wires behind the motherboard, which is very nice.

Leo: Mm-hmm, mm-hmm.

Steve: Yup. I like that case a lot.

Leo: Yeah, we, you know, I'll tell you, I learned long ago, buy a case for its ease of access.

Steve: Yes.

Leo: Because that's something you're going to want.

Steve: It's like in networking, never tie down all the cables because you think it's like...

Leo: You're never done.

Steve: ...you're never going to change anything. You are always going to be changing something.

Leo: Well, good. Our engineers will be happy to hear that because I don't think we have any cables tied down in the basement there.

Steve: No, there's no point.

Leo: But you know what, we're going to be glad because in August we've got to unplug everything and move it. And I have a feeling that this time they will maybe trim it a little bit, make it look pretty. Right now it's a rat's nest down there. Steve, what fun. You know, people don't build PCs that much anymore. But it is really a gratifying thing to do.

Steve: Oh. It is so nice.

Leo: I just look at that machine and think how well, I don't know, OpenBSD would run on that thing. It'd just be - it'd scream.

Steve: Oh, my god. You'd do an "ls," and it would just be a blur. All you'd see is the end. It's like, uh, what happened?

Leo: Where's my listing? No, that's going to be a lot of fun, lot of fun. My friend, we've come to the end of this early. You didn't do a 2.5-hour show. I'm very disappointed. You like Father Robert more than you like me.

Steve: No, we're right on our two-hour mark, which is the sweet spot.

Leo: That's what we want to be.

Steve: Yup.

Leo: Steve Gibson's at GRC.com, and so is so much good stuff, including Steve's super-duper, patented, all-night, nonstop sleeping formula, which by the way, now with Taurine. No, wait a minute, now with L-tryptophan. I keep getting boxes from Steve. Oh, more - rattle, rattle. Oh. So should I eliminate the melatonin now that I've got the L-tryptophan?

Steve: No. The L-tryptophan, I think, just is a nice little additional encouragement.

Leo: Steve, if my liver fails in a year, at least I'll be well rested. And that's how I'm thinking about this.

Steve: I've got to tell you, Leo, there's - and I'm digging in on this. I haven't figured out what it is.

Leo: I sleep. I can't sleep. Oh, I will say this. It is the best jetlag formula ever. So even if you don't want to use it on a regular basis, when we went to New York, I was in bed on time. I was up on time. I was instantly on East Coast time. And Lisa and Michael were, you know, 12:00 noon they're [snore]. But I was up and 6:00 or 7:00, and I was out, I mean, from now on I'm not traveling without that thing. That is great.

Steve: There is something for me that happens after, I think it's about between 8.5 and nine hours. If I go to bed early so that I can get that much, it's almost mystical the next day, how I feel.

Leo: Yeah, nice, yeah. Life is better. Life is better when you sleep.

Steve: It is like - it's amazing.

Leo: Now, have you...

Steve: And I keep - go ahead.

Leo: Have you tried - I'm really tempted to open those capsules and make a little powder that I put in a cup of tea or something. Because it's now up to, like, 10 pills or something.

Steve: I know.

Leo: It's a big handful. And I think it might be better if I had it in a beverage.

Steve: Yeah. I'll be surprised if someone doesn't come along and say, hey, we want to turn this into an all-in-one, ready-to-go package, which would be great.

Leo: Well, soon as you perfect it.

Steve: Yes. For what it's worth, I'm getting a lot of positive feedback. People who have not been able to sleep for years...

Leo: Oh, I'm loving it.

Steve: ...report that they're sleeping for the first time ever.

Leo: Yeah.

Steve: Even, like, college students are saying, hey, this thing works. And it's like, well, I'm just so happy.

Leo: Yeah. Knocks me out, and I sleep through the night, and I feel great the next morning, and not groggy. But we're not selling it. It's just on the web page. It's there...

Steve: Healthy Sleep Formula.

Leo: ...if you want to know about it.

Steve: Just google "healthy sleep formula."

Leo: And of course, while you're there, make sure you get the Never10. Never.

Steve: That is a good name.

Leo: I'm telling you, great SEO. Really, really smart.

Steve: Yeah.

Leo: SpinRite's also there, you know, a good program, too.

Steve: For a while, you know, the other name I was tempted to go with, you know, because we have GWX for Get Windows X, I was tempted to go with FWX. But I thought, no, I like Never10. It's better.

Leo: Good. It's good, but I don't think you'd be in the Sydney Morning Herald with that one, no.

Steve: No.

Leo: Never10 is perfect. So many things there. Just go the GRC.com, browser around. Of course the podcast there, the transcripts. You can get the show from our site, too, TWiT.tv/sn for Security Now!. It's also on YouTube. It's also, actually, if you go to YouTube.com/twit, you'll see all of our shows, and you can subscribe to individual ones. Each of them have their own YouTube channel.

And people keep saying, gosh, I wish you still did the reviews, the Before You Buy stuff. But we do reviews on all the shows, and then we put them on YouTube. And there's a YouTube Product Reviews playlist. So you can, in effect, assemble your own Before You Buy, if you want. And that's really kind of how we've handled that is we've just moved it into this YouTube playlist. But it all starts at YouTube.com/twit.

The newsletter is at TWiT.tv/newsletter. Free. No ads in it, even. I don't know why, but we just decided not to do that. Mainly because our great sponsors make everything possible. We thank them. And we thank you, Steve, and we'll see you next week, Wednesday, I'm sorry, Tuesday, 1:30 p.m. Pacific, 4:30 p.m. Eastern, 20:30 UTC on TWiT. Thanks, Steve.

Steve: Thanks, Leo.