Listener Feedback #188

Description: During this week's Q&A we host a special guest, industry veteran and ISP Brett Glass, who shares his views on the confusing Network Neutrality debate. We also catch up with the past week's security news and answer 10 questions and comments from our listeners.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-457.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-457-lq.mp3

SHOW TEASE: It's time for Security Now!. We've got questions; we've got answers; we've got Steve Gibson. And we're going to begin the show with a debate over Net Neutrality with an Internet Service Provider from beautiful Laramie, Wyoming. Brett Glass joins us, next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 457, recorded May 27th, 2014: Your questions, Steve's answers, #188.

It's time for Security Now!, the show that - sounds like I'm doing a wrestling intro here.

Steve Gibson: You know, your windup gets bigger every week.

Leo: Secuuuuuuuuurity Now!, the show that covers security, now, and privacy, and online stuff. And that's the guy who does it all. I'm just here to, you know, I'm the ringleader. No, he's the ringleader. I'm the sidekick. He does the work. I'm just here...

Steve: Leo, you're the reason that I get dragged into this every week in order to do the podcast.

Leo: Well, I'm proud to say that I dragged Steve here.

Steve: You're the reason this exists.

Leo: We have a good show, really good show planned for you. Every week we talk about security, and then every other week we give you a chance to ask questions. We've got a bunch of questions and answers for you. And a guest.

Steve: Yeah. You and I have known Brett for decades.

Leo: Ages. Ages.

Steve: Yeah. So I would call him an industry veteran of the PC business. He's also an ISP out in Wyoming.

Leo: See, that I didn't know because I know him, of course, by his byline.

Steve: Right, and I think that's where he, well, we'll let him speak for himself after we get him on in the podcast.

Leo: All right.

Steve: But he contacted me because his sense is that he hasn't yet seen anyone explain Net Neutrality correctly. And he said, "I would love to have the chance to do that." And I said, "Well, I happen to have a podcast, so we can make that happen."

Leo: Well, and a perfect guy to do it because he's one of the first, maybe even the very first wireless Internet service provider. He has a WISP in Laramie, Wyoming. A WISP, not a lisp. He has a lisp in Laramie, Wyoming. But he's been around covering this scene since the very, very beginning.

Steve: Yeah. And like us, Leo, he was around before the Internet. So he's lived through the dawn of all of this and watched the PC industry evolve. So he's one of our old-timers, not quite the Jerry Pournelle old-timer, but he's our peer in terms of his experience and background in the industry. So I'm interested to hear his take.

So we're going to talk to Brett. We're going to learn about this week a nifty XP hack that allows you to continue receiving security updates, just like it never got cut off, up until 2019, which gives us another five years.

Leo: That's awfully handy. I'd love to know about that.

Steve: Yeah. We'll talk about eBay's acknowledged fumble from late February/early March, where they lost control of their user database. Couple of Apple security woes. A brief update on where I am with SQRL. And then this is nominally a Q&A episode. So we'll fill the balance of the podcast with as many questions as we can get to.

Leo: It's a jam-packed show today. Leo Laporte, Steve Gibson. And, lo and behold, through the magic of the Internet, Brett Glass is here. Hey, Brett.

BRETT GLASS: Hey, Leo.

Leo: Welcome. Good to have you.

BRETT: Yes, it is great to be here. I've admired your show for quite some time. It's wonderful to be on.

Leo: Well, of course we've been reading you in PC Mag for years. But he's also an Internet Service Provider. Go ahead. You do the introduction. You do the honors.

Steve: Well, and it's funny because, as I was saying, Brett's been around for a long time and understands the way all of this works. Our listeners will appreciate that he was, when we were arranging this, he said, "Well, how do we connect and all that?" And I said, "Well, we use Skype because it's the best solution we've found." And he said, "Oh, there's like a supernode problem with Skype, isn't there?" And I had, I mean, I sort of remembered...

Leo: Not anymore. Microsoft eliminated the supernodes when they bought them.

Steve: Right. It turns out that I was googling to make sure that that had gone away, and it was our podcast, Episode 100-something, where I was explaining about supernodes. And there was something you could do, a configuration switch that would prohibit your Skype client from being a supernode. But anyway, when I got email from Brett, we were arranging to connect before the podcast to make sure that everything was working. And he said, "When I fired up Skype, it started making port 80 and 443 connections all over the world."

Leo: Oh, that's nice.

Steve: "So I've blocked it and given it a single port." So, but my point is...

Leo: But that was the hack. That was what we always did was we said use a dedicated port.

Steve: Yes, yes. And then Skype wouldn't do the supernode thing. But who knows what Microsoft has done. My point is that Brett is savvy enough at the technical end to be a little skeptical and leery of some random conferencing software. And sure enough, he caught the client wanting to go off and do lord knows what. So anyway, that's been neutered.

Leo: Well, thank you.

Steve: And we have Brett direct from Laramie.

Leo: Great to see you, Brett. Thanks for joining us.

BRETT: Yes, well, again, it's good to be here. Should I introduce myself, talk about my background, what I've been doing since I...

Leo: I'm just sorry we made you use Skype. I feel guilty now.

BRETT: Oh, I now know how to neuter Skype.

Leo: Well, there you go.

Steve: Well, so my sense is that you sort of have a pro-Net Neutrality stance, and I want to understand what that is. Or how would you characterize your feelings about this issue and the confusion that people have about Net Neutrality?

Leo: Yeah, but do set us up, Brett. Tell us a little bit about why we should listen to you.

BRETT: Okay. Well, after I was a columnist for InfoWorld for many years - matter of fact, while I was still a columnist for InfoWorld, PCWorld, I also did some work for PC Magazine. I moved to Laramie, Wyoming, and discovered that there really was no fast Internet here. The best you could do was CompuServe at 2400 baud. Not finding this acceptable, I decided that we needed to do something about this, and other people in town were thinking the same thing.

So I went ahead and set up what turned out to be the world's first WISP, or Wireless ISP. We bought radio equipment which had just come onto the market. Lucent was making them. I'd seen the boards at Comdex. We put them together into a wireless network. We connected a lot of businesses and individuals in town who wanted to be on the Internet and have high-speed, and there we were, the world's first WISP.

Leo: That's pretty darn cool. I love that, Wireless Internet Service Provider.

Steve: And you were messing around with Yagi antennas and, like, beaming the stuff from, like, one water tower to the next, like across the state; right?

BRETT: We don't quite cover the whole state, but we do cover the Southeastern corner of the state. We do use these long, herringbone-shaped Yagi antennas. We now use smaller ones. I have one here, as a matter of fact, this little panel that we use now.

Leo: It almost looks like a cell antenna, almost.

Steve: Yeah. But it has a lot more gain than the antenna inside your cell phone. It's a lot more focused. And what that does...

Leo: Is it microwave? What frequencies do you use?

BRETT: We use all of the unlicensed frequencies that the FCC provides. Unfortunately, there aren't a ton of them.

Steve: All of them.

BRETT: Yes. We use 5 GHz. We use 2.4 GHz, which is the original WiFi frequency. We use 900 MHz, which is even older and was the first one that we used way back when.

Leo: Cordless, cordless phones; right? Or no.

BRETT: Yes, cordless phones, power meters, all sorts of different devices use 900 MHz. And now the FCC just about two weeks ago freed up some spectrum at 3.65 GHz, and so we're going to be using that, as well. So we use anything that we can get our hands on without having to pay billions of dollars in licensing fees.

Leo: Like Verizon.

BRETT: Exactly.

Steve: And where do you get - how do you get your bandwidth piped into your central location?

BRETT: That's an interesting story, too. Originally, we had to get it from the telephone company. The telephone company priced it such that its wholesale prices to us were as high as their retail prices when they provided DSL, and we had to find ways of trying to make money anyway, despite the fact that they were raising our costs. Ultimately, we managed to tap into fiber, which is running across the state of Wyoming, and bypass the telephone company. And now we're able to offer much more speed at lower prices.

Steve: Nice.

BRETT: And, by the way, we connect to that fiber using big microwave dishes on the tops of two buildings, one in downtown Laramie and one way out in the countryside where the fiber is. And that's how we connect the two of them together. So we have to be creative. Being a small company, we don't have the advantages of a very large telephone company. So we have to invent our way around the barriers.

Leo: So let's talk Net Neutrality. Now, I think that you've qualified yourself pretty well. You're somebody who's providing Internet service to - how many customers do you have in LARIAT? I mean, Laramie?

BRETT: We have about a thousand accounts.

Leo: So that's a thousand people reliant on you for access to the public Internet.

BRETT: Actually, it's more than a thousand people because behind each account can be hundreds of users. We serve an apartment building, that's one account, but everyone in the apartment building is using it. So we don't actually know how any users we have, but we do know how many bills we send out each month.

Steve: How much bandwidth does this conglomeration consume?

BRETT: Right now we have about 1.25 gigabits of bandwidth coming in through our microwave links.

Steve: Nice. Okay, so Net Neutrality.

BRETT: Okay. Well, the first thing to understand about Net Neutrality is that it's not a well-defined term. When you hear people talk about Net Neutrality, though, there's one thing you can be sure of, and that is what they're talking about is regulating the Internet and regulating ISPs like me, out of the fear that we're somehow going to do something bad to their communications, or overcharge them, or try to do something which is something nasty. And so whenever you hear the term "Net Neutrality," in general what it entails is regulating ISPs under the assumption that we're going to do something bad for consumers.

Leo: By the way, I should point out, I don't think anybody is worried about you, Brett. But the big monopoly ISPs like Comcast may be a little bit more likely to do some of that stuff.

Steve: Well, and so I guess it's the ISPs' control over the so-called "last mile" that makes people nervous because they're the final connector between the Internet and the end-user, the retail bandwidth purchaser, the consumer.

BRETT: Exactly. And people are worried that the ISP will mess with their connection, that they'll spy on it, that they'll restrict it, that they'll hold anything that they can for ransom financially. And that's usually, when you hear people campaigning for Network Neutrality, that's what they're concerned about, and that's what they say. And in fact, though, ISPs have never done that. If you take a look, for example, they talk about censor - they say that they're worried that ISPs will censor. In fact, there has never been an example of any ISP ever censoring legal third-party content. But this idea that they might is enough to get people concerned enough to call for regulation of the 'Net, even though this might have some negative impact.

Leo: I might disagree with you on that, Brett. You've heard of Sandvine.

BRETT: Indeed I have.

Leo: Yeah. It's, of course, a deep packet inspection tool that a lot of ISPs use, and Rogers used, quite famously, in Canada to cut off Skype calls after an hour. So that's an example. And that's anti-competitive because of course Rogers is a telephone company as well as an ISP.

BRETT: Yeah, well, there have been a couple of incidents where certain ISPs have acted in anti-competitive ways and stopped very quickly because the consumers threatened to dump them.

Leo: I'm just arguing your point that nobody's ever had an example of this. There are ample examples, and there are many that are hidden, covert examples that we don't know about because we don't know what people are doing with their Sandvine boxes and the like.

Steve: Well, yeah, and I guess my problem is a lack of choice. I think the argument is, well, if consumers don't like the service they're getting from their bandwidth provider, they can go somewhere else. Well, I mean, I've researched every alternative there is. And, for example, we don't have AT&T U-verse service. There's no fiber near me. I'm too far away for DSL. I'm still using a pair of T1s to get reliable bandwidth to my house. But other than that, it's Cox. It's Cox Cable, and that's the case for typically, like, all the people here. So I guess I'm sensitive to the notion that these major providers, who are continuing to buy each other also, really are eliminating choice from the market because they want more power.

Leo: Also, and I point this out, there's other kinds of issues such as the interconnect issue. And of course we've seen Level 3 talk about how companies like Comcast, in fact five of the big broadband providers in the U.S. - not you, obviously, Brett - use congested ports and refuse to upgrade those until they receive payments. Now, that's not Net Neutrality, I understand. That's not to the edge providers necessarily, or to the home. But it reflects on what I consider their bad will. I don't feel that these big companies - and again, I don't include you in this - have shown any goodwill towards consumers. But go ahead. I just wanted to raise that point before you continue on. So I don't want to interrupt you too much.

Steve: And if I can throw one more thing in, because we were just talking about this a couple weeks ago, the issue with Netflix, for example, which is I think where most people focus, is the idea that the ISP wants money from Netflix because they feel that Netflix is gaining an unfair advantage and profiting from their sort of common carrier, currently neutral handling of bandwidth regardless of its source.

BRETT: Ah. Okay. You've raised a lot of concerns, you know, a lot of topics all at once. I'll try to address them one at a time and talk a little bit about, not only from my point of view, but the consumer's point of view, because I'm an advocate for my customers, what

this all means. Yes, you are correct that in some cases you've seen some attempts at anti-competitive actions on the part of ISPs. The first, the most prominent example being a phone company called Madison River, which blocked VoIP over their network. They only did this for about a month, though, because the outcry from consumers was so great that they stopped.

Again, whenever you've seen an attempt at an anti-competitive strategy, it's been very short-lived. And one thing, again, that you've never seen, and this I think is a key point, you've never seen censorship. At most what you've seen is attempts to advantage a service which the broadband provider provided that was in competition with a third-party service it rode over the top over the Internet. The good news is that these attempts to do such things have always historically lasted a very short time and, even without action on the part of the government, have gone away very quickly as the consumers have threatened to raise a ruckus and threatened to switch.

Now, as to the point of competition, you're right, there should be more competition. But the worst way to discourage competition is to regulate in a very heavy-handed way. Some of the regulations which have been proposed as a part of Net Neutrality would actually put companies, small companies like mine, which are competitive, we compete with the cable company and the telephone company, out of business because we couldn't handle the burden of the regulations. And then you would have less competition rather than more, and there would be more of a temptation for a very large company to misbehave because they'd realize that, well, there's no place that you could turn to.

Right now - when I started my WISP back in 1992, as far as I know I was the world's first. There are now 3,000 of us all over the country. And that's quite a lot, if you think about it, and quite a large number per state. Not everyone has access to one. But something like 80 to 90% of the U.S. population has access to a WISP right now. If we want that to grow, if we want there to be still more competitive providers, we want to be very careful about how we regulate because, if the regulations make it tough to start up a new business, if it makes it tough to make a profit, then you're going to have fewer and fewer, and only the large companies that have other sources of revenue, like the cable companies which provide you with TV, are going to be able to survive.

Now, you also talked about Netflix. And that's an interesting situation for our ISP in particular. Our bandwidth is very expensive. And because we use wireless, the amount of spectrum that we have available to us is very limited. And so people watching Netflix - and believe me, this is the first thing that they ask us about. Whenever they call and they ask for service, they say, "Can I receive Netflix? Can I stream Netflix in HD?" Very first question. They will not subscribe to your ISP if you can't provide that. Right away they want to be able to do that. And so it's something which you must do as an ISP.

Netflix has the market power here. If Netflix were to refuse to serve our customers or somehow disadvantage our ISP, they could do bad things to us. They could basically deprive us of a lot of our customers, not the other way around. We don't have a choice. We must carry Netflix. We must make sure that the quality is good. They have a choice. They can afford to either serve us well or not. And in fact...

Leo: Why wouldn't they serve you well? I mean, that's saying we don't want the customers' business.

BRETT: Well, here's what's going on. Netflix recently went to Comcast, a very large ISP, and they agreed to pay them money to connect directly into their network,

instead of going through a content distribution network like Level 3 or Akamai, go directly into their network to provide higher quality service to their customers. And they actually paid Comcast money to build this out, this facility, and so it could happen. And so Comcast customers are getting a special deal from Netflix.

Well, I went, and I called up Netflix, and I said, "Okay, well, I've got an ISP, too. Will you do the same thing for me?" And they said, oh, no, we're not going to do anything like that. You are going to have to pay thousands of dollars per month to run a special connection to us, and then host one of our servers in your facility, which is something that ISPs normally charge for. And then maybe we will do the same thing for you that we do for Comcast.

Leo: So they didn't deny you access to their Open Connect.

BRETT: Well, that's what Open Connect is. What they call Open Connect.

Leo: They said that you have to connect to Open Connect. But...

BRETT: They said that I would have to pay, that I would have to shell out money to do it.

Leo: To Netflix?

BRETT: Not to Netflix, but I would have to pay for all of the facilities, and Netflix wouldn't pay me anything, whereas Netflix is paying Comcast. So you see, when you're a little guy...

Leo: And you're saying you can't pass that along to your customers because they wouldn't accept it.

BRETT: That's right.

Leo: So it seems to me the problem is that your customers are saying we're not going to pay for the service we want.

BRETT: Well, the customer ultimately pays for...

Leo: That's your problem.

BRETT: The customer ultimately pays for everything anyway. All of the costs wind up coming back to the customer. The question is, of what's left, who gets to keep which

part? And this is what's going on, really going on with Netflix. Netflix, and also to a certain extent Google and Amazon and all of the other large content providers, have set themselves up in a tug-of-war with ISPs over who is going to get what share of the total amount of money that the customer is shelling out for their Internet connection and for the content.

Now, if we want to be fair about this, okay, if you think about this in terms of fairness, basically people should pay in proportion to the resources that they use. Ultimately the customer, the Internet customer who is streaming 24 hours a day should pay more for that than the one who just uses the web and email. I think we can all agree to that.

Leo: We can all agree on that. That's not the issue, of course, yeah.

BRETT: Yeah. And most people would also like their monthly bills to be predictable and fixed. People hate caps. They hate overage charges. They hate surprises. They really want to pay a fixed amount per month for everything, whether it's their ISP bill or their bill to Netflix or whoever. And so how can you make both of those things happen at the same time?

Well, just simple arithmetic, you don't know which ISP customer is going to be the heavy streamer and which isn't. And so one good mechanism by which this could be done is what's called a "two-sided market." This is something there's been a lot of fuss about. You'll hear a lot of talk about this. The two-sided market is sort of like a newspaper, where the cost of the newspaper is borne in part by the subscriber, who pays to get it delivered, and part by the advertisers, who pay to get it printed, and also as the paper gets thicker they pay more and more to cover the increased costs of printing it.

Well, you can have the same thing in the Internet. People can pay a fixed fee for their basic ISP connection. And then if they decide to stream day and night, what they can do is they can pay a fixed fee to the content provider, like Netflix, and then Netflix can pay a little bit of that back to the ISP to cover the extra resources that all of this streaming takes. And then you've met all the criteria that the customer wants. You have fixed fees, and everything gets paid for, and it's fair. But what you hear from the Network Neutrality advocates, they scream when they hear this, oh, no, the ISP is asking for ransom.

Steve: Yeah, I can see how that flow of money makes sense because, rather than the ISP being responsible for bandwidth billing per customer, essentially Netflix is already charging their customers for their use of content, and so you just sort of change the way the money flows.

BRETT: Exactly. And the way the money flows in the end winds up being fair because the only people who are paying more than they would pay for their basic Internet connection are the people who are signed up for Netflix and are going to be using the extra bandwidth.

So the chairman of the FCC, Tom Wheeler, went ahead and proposed that, when they made some new rules to try to keep ISPs from misbehaving, they allow what's called "two-sided markets." And immediately there was this tremendous hue and cry that

you're hearing all over the Internet: "Oh, no, that's creating a fast lane. That's somehow unfair." Most of this was actually the result of lobbying by Netflix and Google, who simply didn't want any of the money to flow back from them to the ISPs. They wanted to keep it all. And so when you hear people talking about that, that's, you know, a lot of it is due to the publicity campaigns by the content providers that want to keep more of the total money that the customer is paying.

Steve: That does make a lot of sense, Brett.

Leo: Not to me. But I'd like to jump in. It makes no sense at all.

BRETT: Please.

Leo: What you're saying is of course you want to make more money. I don't blame you. That's exactly what Comcast wants to do, and so does Google, and everybody else wants to make more money. What doesn't make sense is for you to undercharge and then draw more money from the provider. You need to charge what your service costs you. And the problem is not Netflix, which can afford it, or Google, which could afford it, but TWiT, which can't afford it.

So what you're telling me is that, if I wanted access, and your customers were downloading a lot of TWiT, I'd have to give you some money. That's not how the Internet was designed, Brett. You know that perfectly well. It was never designed for edge providers to pay Internet service providers. You're a utility. You provide a utility. It's as if the water company says, well, you're drinking an awful lot of water. We're going to have to figure out some way to get some money from the reservoir. Your job is to provide free access to the Internet. Why is that not your job?

BRETT: Well, we're in business to make money, but we're not interested in making it unfairly. We're interested in earning our keep. But on the other hand, we can't - because bandwidth costs money, there's no way that we can afford to give an unlimited amount to any one person. If they stream 24 hours a day, that's going to cost more than - this is going to cost more than they're paying.

Leo: Well, you need to charge them for what they're using. Nobody's saying you can't do that. What they're saying is you can't go to Netflix or TWiT and say, hey, by the way, our customers are using too much of you. Can you pay us some?

Steve: Right. So that's the point that Brett was making when he laid the foundation, saying that customers want to pay a fixed amount. And so if the ISP isn't going to get additional revenue from customers based on their usage, the alternative model...

Leo: Well, then they are - that's not going to work. Sorry. That's not a good alternative model.

BRETT: So Leo, what you're saying is...

Leo: What I'm saying is you cannot be biased about what content you bring your customer, just because the customer says, well, I'm not willing to pay for my service. You charge more to the customer. That's fine. You charge...

Steve: It's not really what content, it's how much content. And so, I mean...

Leo: It's not. It's not. No, no, it's not, because it's very specific to the provider.

Steve: No, the model is very much like electricity. We know that, if we leave air conditioning on all the time, if we use more AC, we're going to get a larger bill at the end of the month.

Leo: Yeah?

Steve: And right now that is not the way Internet bandwidth works. And so what we're saying, I guess what you're saying, Leo, is that in order to keep this being a free ride for the content producers, then the consumers will have to pay based on the amount that they use. Which, I mean...

Leo: Understandably. But the issue is so who has to pay for that, then? In other words, you're telling me that, unless I have enough money to give Brett some money to have access to his customers, I don't get to exist on the Internet?

BRETT: That's not what anyone's saying.

Leo: What are you saying?

BRETT: Okay.

Leo: If somebody watches TWiT 24/7, do you get to charge me?

BRETT: Actually, TWiT uses a lot less bandwidth than Netflix. Netflix tends to be a bandwidth hog.

Leo: But let's not use - I understand, but let's not use Netflix as an example. Let's use TWiT as an example. That's who the issue is, is that not all service providers are alike; right?

BRETT: Exactly. And the ones that impose the heaviest burden are the ones that probably should be participating in feeding some of the revenue back to cover the resources that they use. And again, this is...

Steve: Well, okay. So...

Leo: But that is fast-lane access.

BRETT: ...[indiscernible] to the consumer. So I'm not being - oh, I'm sorry. Go ahead.

Steve: It seems really clear to me that one of the problems we have is that consumers don't really understand the notion of bandwidth. They haven't been trained. They haven't been taught. They don't get that, like, texting uses no bandwidth, and watching a movie is completely different from texting or web surfing. So they're just - there isn't that notion. And so it seems to me that some of this is consumer expectation, which right now consumers have been pampered. They've been able to do pretty much everything they want to. But the system is getting stretched because the nature of what people do with the Internet has dramatically changed in the last few years. And Netflix is like the poster child for the driver of this change, is suddenly now, hey, you know, we want to be cord cutters. We don't want to have to watch television when it's being broadcast. We want to just get it whenever we want it.

Well, there is a real bandwidth cost for providing that flexibility, which at this point consumers have been insulated from. And so, for example, Brett, you're saying consumers want a fixed-price bill. They don't want to pay extra based on their conduct. They just want Internet connectivity. Yet what they're wanting to do is dramatically more expensive now than it was pre-Netflix. And so the model that the ISPs have come up with is, in trying to keep the consumer from having to pay as they go, or pay for their actual usage, is to get the money which this bandwidth actually costs from the providers.

And, I mean, I can see the elegance of that solution because the providers have accounts with their consumers. Netflix has customers, and the customers are paying for the bandwidth, essentially. And the alternative is Leo's model, where the providers are never charged for the fact that they're just offering this content. But that means then that the end-users have to be charged on a variable basis for how much content they use.

BRETT: Exactly. And either model would work. But the consumers strongly prefer to have fixed bills. It's sort of like, I mean, let's go back to the analogy of the newspaper. When you get a newspaper that's thick with ads on a particular day, it's going to vary on different days. You don't pay a different price for your subscription. Your paper boy doesn't come and say, well, your papers weighed more this month. I'm going to charge you a little bit more. What happens is the advertisers, the content providers in that context, make up the difference when they pay for those additional ads. They pay for the additional cost of those papers. And the consumer really likes this, and the advertisers think it's fair, too.

What's happening here, though, in the Internet ecosystem, is that companies like Google and Netflix are refusing to be the conduit for that. And but then, well, okay, there's a legitimate argument as to how you want to do this, as to how you want to get the bills paid and keep the Internet on. But what they're doing, instead of coming out and saying, okay, we have a controversy here, we have to figure out how we're going to make this - get everything paid for. Instead, they're demonizing the ISPs, and they're claiming that the ISPs are evil, are asking to be paid to deliver more services, and that's what's not fair.

Steve: I guess we've sort of seen a half-step in the way cell bills have been arranged,

where there are similar constraints. There's a limited amount of bandwidth which a certain customer base has to share. And so there are bandwidth caps and variable plans which you use in order to try to match your consumption with a model that makes sense for the ISP. And this is why I brought up the idea of electricity, because consumers are actually used to paying a variable amount for their electric bill every month. And at this moment there is no variability in what we pay for bandwidth to our ISP, but there is in the electricity that we use from our electrical utility provider.

Leo: And of course I pay - the problem is not that I am not paying for my access to the Internet, or Google or anybody isn't. We're all paying...

Steve: Right.

Leo: ...for access to the Internet. We pay through the nose for our access to the Internet. It's that we don't want to have to pay the ISPs, too. It doesn't make any sense at all, Brett. You want us to shoulder a burden that you're unwilling to shoulder. You offer, as an Internet service provider, free and open access to the Internet. Do you not?

BRETT: Yes, we do.

Leo: Well, that's your offer. And it's got to cost you what it costs you.

BRETT: Well, bandwidth costs money.

Leo: I know. I pay for it. I have to pay you, too?

BRETT: Well, yes. It costs a tremendous amount of money to do this. We pay, you know, until a couple of years ago, we were paying $100 per mbps per month for our bandwidth. When we made our direct connection to the Internet, managed to get that cost down. We still wound up paying $20 per mbps per month. And that, you know, that's a good price when you're out here in a rural area. This really costs money. And in order to keep the lights on, we do need somehow to cover the costs. Wherever that money, whatever revenue model you arrange, whether some of it flows, you know, whether the customer pays for all of it, whether there's a meter running, whether there's a cap, whether some of it is fed back through the content providers, you certainly - you just need a certain amount of money to keep the lights on, for me to be able to pay my employees.

I'm not being greedy here. I'm just trying to make the books balance, or I have to shut things down. So I'm not trying to be unfair. I don't think it's fair to demonize me for doing that. I'm open to different models. But what isn't going to work is to stretch the ISP farther and farther to the point where it can't stay in business.

Leo: Well, and my big concern is, as we all know, an open Internet is what's created

so much innovation and progress. And my problem is I do pay. I pay for everybody who watches every show, everybody who downloads every show. The cost is not negligible. We pay, of course, our provider. I'm not sure why I should support you and your business. Your customers need to pay a fair price. And the problem is not so much that, I mean, I don't know how I would pay every Internet service provider for access to their customers. You want to charge your customers for access to the Internet, and you want to charge me for access to your customers.

That sounds like you've got a crappy business model, Brett. It's not my problem because I, be honest with you, I can't do it. And what you're going to do is you're going to shut down every small content provider because every ISP comes to them and says, "Hey, would you like access to our customers?" And by the way, your customers are not going to be very happy, either, because all they're going to get access to is the big guys. So it seems to me that your business model is flawed, Brett.

BRETT: Well, unfortunately, Leo, while I've created a lot of technology that provides the service, I didn't create the business model for the Internet. That was something which I kind of had to adopt and go along with based on what resources were available to me and what customers want. And I understand your point of view and your position very well. Ultimately, to some extent, of course, it's your advertisers who are really paying the bills for you, of course, and they're paying to reach the customers. And they may or may not be willing to pay for extra bandwidth, whatever.

Leo: Well, let's not use me, then. Let's use the Electronic Frontier Foundation as an example, or a nonprofit that wants to be on the Internet, wants to use the Internet, and it's been used very effectively to organize, to raise awareness. You're saying that any company that wants to be on the Internet should have to pay for access to people at the other end?

BRETT: Well, someone should pay for it, Leo.

Leo: Yes, your customers, because that's what they're paying for.

BRETT: And again, my customers do pay a fixed fee per month. And that gives them a certain amount of access, whether or not the content provider is paying. If they want to access a nonprofit, whatever, the Red Cross, any nonprofit in the world, that will get them there. But when we're talking about very high-bandwidth, high-profit material such as things like Netflix, then in order to do that, because it commands so many resources, one way to do that is to have a business model where revenue comes from the other side. Again, we could do it by billing the customers. We could do it with caps. There is a site out on the Internet, though, which expresses tremendous frustration with that. Have you ever been to the StopTheCap website?

Leo: Yeah, no, I understand that. And maybe customers are expecting too much, or maybe ISPs aren't willing to tell the truth to their customers. Yet I see so many

countries like Scandinavia, South Korea, where they get ample bandwidth for very low costs. We pay an awful lot in this country for our access to the Internet. Why is that?

BRETT: Well, we're a bigger country. Geographically we're much more spread out. Someplace like Korea, it's very easy to provide high-speed Internet access to everybody, extremely high speeds, although in fact, if you look at the numbers, they're claiming gigabit access. In fact, most people never use anywhere near that much. The sum total of all of the human census combined is about the bandwidth of a T1 line.

But in fact we have a large and difficult-to-span country. I have only one choice right now of fiber providers that I can hook to. I'm working right now on building hundreds of miles of microwave dishes out so that I have a second choice. And that costs money. And ultimately, like I said, I'm not trying to profiteer off of this. I'm just trying to pay the bills. Ultimately, the cost of doing that has to come back to the consumer somehow.

So I think what we're seeing here is that one of the things that Network Neutrality is really about is not so much the idea that people are going to censor, but just how do you structure a business model that's fair to everybody and works for everybody and doesn't exploit any one of the businesses that's in the chain between the person who creates the content and the end-user. And it's a legitimate policy. I just wish there wasn't so much acrimony here.

Leo: Yeah, and I understand. I just feel like the risk, the very real high risk, however benevolent you feel that Comcast is, is that the Internet as we think it was, maybe it wasn't ever designed this way, but I always thought of the Internet is the idea was that bits can travel freely, openly, to any other point on the Internet. And the benefit to the country and to the users and to society is that all kinds of speech can be heard; all kinds of innovations can be created, like Skype. And I worry very much that Comcast is not the benevolent company that you seem to think it is. I'm not worried about Brett Glass's ISP. I'm sure I don't have to worry about LARIAT. But I worry a lot more about Comcast.

I think you're wrong when you say there's no history of misbehavior. I think there's a long and checkered history of misbehavior. And I think that - now, and I also understand, and I would guess that you have a political bent that is against government regulation in general. And I understand people's reluctance to let the government get involved in any way on the Internet. But I feel the government has created this problem by creating a lack of competition. Maybe the solution is to foster competition as opposed to regulate Net Neutrality.

Steve: Well, and I really do think we're going through an interesting phase where we're talking - what we're seeing is the - and we've discussed this on the podcast in the last few weeks, the notion of the commercialization of the Internet. This was something that the three of us created, effectively, decades ago, and sort of nursed and watched and fed, and we used email and brought this thing to birth, essentially. And to me it almost seems inevitable that this is going to end up going commercial, that the Internet is going to be turned into various forms of business. I mean...

Leo: Tim Wu says it's a pendulum that swings between oligopoly and community. Brett, do you think that community Internet is a viable alternative to this?

BRETT: Well, that's an interesting point, Leo. When I started...

Leo: In a way you've created one, haven't you.

BRETT: Well, as a matter of fact, when I started LARIAT back in 1992, I started it as a nonprofit. It was a nonprofit rural telecommunications cooperative. And it ran that way for 10 years. After the 10 years were up, the members of the cooperative decided that they would rather buy from a private company that could get investment, that could go out and do some things that it was tough to do with a nonprofit. And most of all, they didn't feel like they were competent to really manage the thing. They weren't techies. And they didn't like the idea of being members of a co-op where they really didn't even know, you know, they had a vote, but they didn't even really know what to vote for. They just wanted to pay for a product and have it be a good one. They wanted to have a choice of people to go to, if possible, for that product.

So in a way our users decided that, rather than have this be a communal resource, that they wanted to encourage entrepreneurship. They asked me and my wife if we would take it private, and so we did. And the privatization of the Internet, by the way, at that point was well underway. It started in the early '90s. And the moment, as a matter of fact, companies began getting on the Internet left and right, it became inevitable that it was going to become privatized.

What the Internet became in the early '90s, and, you know, this was the vision, was that it would be a federation of privately owned networks that agreed to work together out of mutual self-interest. It's a very heterogeneous federation of networks. It's full of, you know, people talk about slow lanes and fast lanes. Well, it's full of fast lanes and slow lanes and in-between lanes and back roads and special detours to try to get things to certain places faster. That's just the way, you know, that's the way the Internet actually has always been.

People talk about the idea of fast lanes and slow lanes as if it's something new, and the Internet has always had them. It's always had prioritization for certain kinds of traffic, for instance. Yes, it's chaotic. Yes, it makes things less predictable. It's certainly less predictable than the Bell system was when it guaranteed that your phone call was going to go through. But this chaos has led to wonderful things. And before we restrict it too much, we need to think about whether we're going to lose the benefits of this chaos, this creativity, and, frankly, this entrepreneurial drive that people will have in the hopes of making some money.

Steve: Well, and Leo, when you talk about regulation, you're talking about the government preventing these sorts of deals; right? I mean, enforcing neutrality.

Leo: Well, I think the subtext of this is that a lot of people who wish the FCC would protect an open Internet believe that the FCC needs to adopt Title 2 of the Telecommunications Act, which would classify Brett and every other broadband

provider as a telecommunications service.

Steve: Common carrier.

Leo: A common carrier. And I understand that Brett doesn't want that. I don't blame you. Although there isn't any evidence of how the FCC would enforce these rules. I mean, they're not required to enforce all the telecommunications rules.

BRETT: Actually, yeah, Leo, actually I can speak to that, as well, because it's kind of interesting. Title 2, if you read Title 2 of the Telecommunications Act, all you need to do is go online and type in the following thing, the following term into any search engine. Type in "47 USC 201." That will get you to the beginning of Title 2 of the Telecommunications Act, and you'll start to read.

And one of the first things you'll see, the first couple of paragraphs in, you'll start to see that it talks about different kinds of telecommunications, how to classify the traffic according to who is calling whom and prioritizing it and charging different amounts for it, all of the things that the Network Neutrality advocates don't want, and that are built into that law. Once you adopt it, there are some parts of the law that the FCC claims it can ignore. It can't ignore that part. That part's mandatory. Basically what Title 2 does is it regulates, it would try to regulate the Internet as if it was a 19th-century telephone company.

Leo: Right.

BRETT: The rules don't fit at all. And while some people say maybe we want something, a little more responsibility on the part of ISPs - and I don't object to that, you know, because we now are filling a more and more important role in society. Title 2 is so wrong for this. As I said, two or three paragraphs in you'll realize this is not the right way to go. If we're going to do something, it should be de novo, and it should be designed for the Internet.

Leo: I agree with you on that. Unfortunately, I don't think we're going to get any of the above. But I'm really glad you could come on, Brett, and make your case, especially as somebody who is on the ground with this.

BRETT: I'll be climbing on a customer's roof this afternoon, as a matter of fact.

Leo: Or on the air.

BRETT: Yes. And unlike the big guys like Comcast, I actually meet every single one of my customers. So I'm really - I'm actually, when I speak about all of this, I'm not speaking about this from the point of view of a large corporation that's out to make money. I'm searching myself to try to find out what the best thing is for my users. And all I can say is, when you hear the term "Net Neutrality," don't think that it's

simple, and don't think that there are really any black hats and white hats.

Leo: I think that's clear. I think you've made that very, very clear. And I certainly want you to be able to do what you're doing because I think it's very important to the community. You are the choice for the community. I think maybe the community doesn't understand how expensive it is to do what you want to do.

Steve: I think that's exactly the case. And the other thing that really...

Leo: And I don't want you to cost me because your community doesn't get it, or they don't want to.

Steve: The other thing that's so frustrating for Brett is that he'll have a hundred different people, all streaming the same content at, like, overlapping or similar times, or even at different times. But there's this huge amount of very expensive redundancy right now in the way this is set up which is, from my technical standpoint or thinking, is why it's so compelling to think about caching the expensive content within the borders of the ISP so that the first customer to get it brings it in, and then you have it locally for all the other 99 people who want to watch the seventh season of "Mad Men."

BRETT: Yes. And, Steve, you'll notice I'm nodding. I think you are absolutely right about this from a technical standpoint, and I have besieged Netflix with emails and telephone calls saying, "Why can't you let an ISP cache your content? I am willing to go out and buy a huge machine with tons of disk drives to do exactly that." They will not let me do that.

Steve: Oh, interesting.

Leo: Yeah, well, that's probably Hollywood won't let you do that, I would guess.

BRETT: They claim that their technology was not set up to allow it.

Leo: Oh, interesting.

BRETT: And in fact they're violating Internet standards because Internet standards actually say that static content that's repeatedly sent over the Internet ought to be cacheable. But they don't...

Leo: That's puzzling, yeah, that's puzzling because I believe Apple uses Akamai to cache Netflix content for Apple TVs and stuff.

Steve: Well, and the term you used for that Netflix service is that; isn't it? I thought that that thing that ISPs do where they install Netflix gear in their datacenter...

Leo: The Open Connect plan.

BRETT: Yes.

Steve: Yeah.

BRETT: Actually, Open Connect is not a cache. Open Connect is a server. It actually gets loaded up with all of the content, whether or not anybody streams it. So it doesn't save as much as a cache would. A whole lot of stuff gets transmitted to that server...

Steve: So it's a big mirror.

Leo: Oh, that's interesting.

BRETT: ...that's never used.

Leo: That's not good. Well, unfortunately, I know how hard this is. We're going to move along because we can only take three or four hours for this. And I know how hard it is because as soon as Brett came on, Larry at DotNet went down. You might want to go check your servers because we've probably just crashed your site.

BRETT: Well, believe it or not we're working over - right now, as I talk to you, I am Skyping over wireless right now.

Leo: Good. You've had an excellent connection.

BRETT: So the wireless must still be up.

Leo: Yeah. It's working quite well. Yeah, yeah, just the website's down.

Steve: Brett, thank you so much. This was really good.

Leo: Very interesting stuff.

BRETT: Yes, yes. Leo, Steve, it's been fantastic. Let me know if there are other conversations about anything to which I can contribute.

Leo: Don't send me a bill for your website, though;, okay?

BRETT: I promise I won't do that.

Leo: Thanks, Brett. Take care.

Steve: Thanks, Brett.

Leo: Well, we have a lot more to talk about. Steve Gibson, Leo Laporte, and thanks to Brett Glass. Really interesting stuff to have Brett on. Steve, what do you want to do? You want to do your headlines here? Or I don't know how many questions we're going to get to.

Steve: Yeah, we'll just - we'll get to as many as we get to.

Leo: We'll do what we do. Okay.

Steve: Yeah. I wanted to share something that really hit the news and was interesting in the last week, and I think people tweeted it to me just because everyone understands my stance. But I first saw this from Matt Graham's blog. It's GrahamLabs.com. And the URL tail is "embedded saves the day." So, and I imagine if you just go to GrahamLabs.com, it's the most recent posting. And Matt doesn't take credit for this. He recognizes that he stumbled upon it as he was like sort of - in the way the world works now, where there's sort of this group conscience of things that are happening.

And what came to light in hacker forums that Matt reported and then ZDNet and BetaNews and others have all picked it up and confirmed it is, yes, is that the point-of-sale versions of Windows XP do not have their updates cut off as of last month. Those continue till 2019, another five years. So the cash registers and the ATMs, which are using Windows XP Embedded, are not in trouble because they continue to get updates. The question, then, is what's the difference?

And it turns out there's a lot of difference, but there's only one thing significant, and it is one registry entry. Anyone who's running Windows XP can add a single registry entry, and Matt lists it, and ZDNet, their article, it's Larry again who did a piece, "Registry Hack Enables Continued Updates for Windows XP." I'm sure you can find it that way. So you turn this into a text file and name it .reg. Double-click it, it'll confirm - and this is for Windows XP only. It'll confirm that you want to enter this into the registry. It adds under the HKEY_LOCAL_MACHINE\SYSTEM key under WPA. It's a key, PosReady. And it sets a value of "installed" to one. Essentially, now your own Windows Update and Microsoft think that your version of Windows XP is Embedded, and you now continue to receive security updates.

Leo: And please don't contact me if it breaks Windows, which it will.

Steve: Well...

Leo: Which it will because you're going to download an update that's inappropriate, and you're going to be - so Microsoft says: "Windows ... customers ... run a

significant risk of functionality issues with their machines if they install these updates ... they are not tested against Windows XP."

Steve: Okay.

Leo: I mean, of course they're going to say that. But I think that actually probably could be the case. Right?

Steve: My guess is that this will work just fine because in fact they are essentially the same operating system, and they've been receiving all of the same security updates up until now. And we know that Microsoft is continuing to provide Windows XP updates under a paid plan for people who want extended updates. My guess is that this won't last long, that Microsoft will produce an update which updates this out of existence. But for the time being, I thought this was an interesting hack.

Leo: I'll read you the Microsoft statement which they provided for ZDNet, just so that we don't - we're off the hook here: "We recently became aware of a hack that purportedly aims to provide security updates to Windows XP customers. The security updates that could be installed are intended for Windows Embedded and Windows Server 2003 customers and do not fully protect Windows XP customers. Windows XP customers also run a significant risk of functionality issues with their machines if they install these updates, as they are not tested against Windows XP." They say the best way for you to protect yourself is to "upgrade to a more modern operating system, like Windows 7 or Windows 8.1." Now we're off the hook, Steve. You may proceed.

Steve: All right. So...

Leo: By the way, that's Larry Seltzer, our friend Larry Seltzer writing that one.

Steve: Yes, yes. So eBay lost control of their user database. They're saying it was late February and early March.

Leo: Yow.

Steve: And then it went unknown until two weeks ago when last Wednesday they posted the news. And I didn't see any numbers. So normally we get numbers that are sort of dramatic, like how many hundreds of thousands of people this represents. I think this is just "all."

Leo: Which is 145 million. All is 145 million. And they gave us no reason to think it wasn't all, frankly.

Steve: Correct. There was no division, or if you'd only logged in in the last year.

Leo: Some customers or, yeah.

Steve: Right, right. So this is customer names, encrypted passwords - we'll come back to that phrase - email addresses, physical addresses, phone numbers, and dates of birth. So definitely highly sensitive information that was lost. You know, names, email addresses, physical addresses, meaning your ship-to addresses and phone numbers and so forth. They specifically said this does not include financial information. So your credit card stuff is in a different database that presumably was not hacked. And there has been, they're saying, no evidence that any of this has been used.

So it's not clear what evidence they would have because a lot of this is real-world material, not just cyber material. And they've never given any clarity to what "encrypted passwords" mean, you know, how are they salted, what algorithm used, what size they are, and blah blah blah. What did raise a lot of ire was that - so the consequence of this was eBay sending out email - it took me a long time to get mine. I was curious to see...

Leo: I got mine today.

Steve: Yes. I got mine yesterday. So, and this rollout of email began last Wednesday. So, yes, it takes a little while to get 145 million pieces of email out.

Leo: I guess so.

Steve: And the technology isn't very mature. There's a banner posted on your eBay account when you log in, and even before you log in, advising you to change your password. But it doesn't know whether you have or not. So even after I did, because I've had the same password - the good news is this was back in the era where I had a handful of passwords, and it's one that I hadn't changed because I by some coincidence never used it anywhere else. And it was a good password, but it was short. So I took the opportunity to make this as long as possible.

It used to be that there was no upper length limit on eBay passwords, and I heard from some of our listeners who had 64-character passwords, which are no longer accepted. eBay now requires an 8 to 20-character password for whatever reasons. Just seems arbitrary to me. But for what it's worth, 20 completely random characters with upper and lowercase and special characters thrown in, all of which eBay accepts. In fact, they have a requirement for passwords to have some of that junk in them to make them stronger. That's really going to be all the strength you need.

So, again, I think people are a little annoyed at any length limit because we know technically there need not be any. And in fact I'm stepping on one of our Q&A questions, I just realized, because that's where I got some of this was from someone telling me of his experience. So we'll get to that here in a few minutes. So anyway, that's that news. Anyone who's used eBay, probably who has ever had an account, either has recently or will be getting email telling them, oh, you ought to change your password. Even though we don't know of any mischief that anyone has gotten up to, the passwords were encrypted in a way we're not disclosing, still we think it would be a good thing for you to

change your password.

Leo: I just feel like there's so much we don't know, that they're just not telling us anything.

Steve: They've said very little. And it's never good news for anyone when they're saying, sorry, everyone who uses us has to change their password.

Leo: The real issue is people who use the same password in multiple places.

Steve: Yes, and they do, in their blog post, and in the various news stories, remind people of the nightmare which is, we've been saying that for years, it's really unsafe to reuse the same password in two locations, which then of course transfers all the burden onto the user until we get to a world where we no longer need passwords, which we'll be talking about here in a minute.

Just this morning the news broke that Australians woke up to find their iPhones, iPads, and Macs locked. Did you guys cover this on MacBreak?

Leo: Yeah, and I don't think it's - I think it's...

Steve: It seems like a small thing.

Leo: Very small.

Steve: Yes, not like it's, like, everything.

Leo: Like a handful of people.

Steve: It looks like - yes. And also, I mean, there are a couple curious things. First of all, the hacker goes by the name Oleg Pliss, O-l-e-g P-l-i-s-s. And he wants people to send him between 50 and $100 through his PayPal account, to hotmail address lock404@hotmail.com.

Leo: Well, a couple of things on that. Oleg Pliss is a well-known programmer at Oracle. It's not the guy's name, obviously. And PayPal says there is no such account. So they're not really asking for money because there's no way to give them money.

Steve: Well, and PayPal is the last place you would want to be sending bootleg malware ransom through.

Leo: You can't. And the good news is you can't send them any money. So we decided on MacBreak Weekly that it's likely there was some other issue somewhere, perhaps could have been the eBay thing, where somebody used the same password on iCloud as they used on eBay, something like that. Somebody tried a few, and it worked.

Steve: So here is the takeaway, though. Because if you did not have a password on your devices, then this small hack - and again, really, Leo, it's not like it's hundreds of millions of people. It's some people. They found an unknown passcode, unknown to them, had been added to their device, which prevented them from doing anything. People who had previously installed a passcode on their devices, so needless to say that's all Security Now! listeners, you're able to restore from a backup in iTunes, and you're okay. So for those who did implement security on their devices, you're able to get yourself back up on your feet without any problem. And it's not clear, actually, unless you know more, about what people do whose phones are locked with a passcode they don't know.

Leo: There's nothing you can do.

Steve: They can just wipe them; right?

Leo: Yeah, restore it from your backup.

Steve: Wow. And then in an interesting bit of synchronized news, Apple had a little trip over their feet this weekend. The swscan.apple.com SSL certificate, which is required to do software updates, expired on Saturday, and software updates broke.

Leo: Whoops.

Steve: And sure enough, I put that domain name, swscan.apple.com into my favorite certificate testing site, Digicert.com/help, and also SSL Labs has the same sort of facility. And, yep, the certificate is now valid from May 25th of 2014, which was Saturday, or I guess Sunday, to May 24th of 2016. So they have a two-year certificate which was minted in an emergency mode immediately upon someone realizing, whoa, that one got away from us. And it's a Symantec cert which is signed by VeriSign. So there's like a four-certificate chain of authentication in there from VeriSign as the CA, then to Symantec, then to Apple, then to this end cert. So, interesting.

I'm continuing to make great progress with SQRL. I just finished addressing, after putting the whole entropy issue to bed, I just finished redesigning SQRL's secure storage system. I had quickly cranked one out many months ago when someone needed it, somebody who was implementing their own client. And I made it very clear this was all provisional. But now I need to use it. And I looked at it, and I thought, okay, this no longer really makes any sense because I have a much better sense for the context of its application.

So in the last three days I redesigned that, posted the spec, updated the web page at GRC. Anyone who's curious might find it interesting. It's a nice little walk through some

computer science where I've designed an extremely lean data representation which is also extremely expandable for the future, not loaded with lots of metadata, like JSON or XML. It's a binary-friendly format because we want to be able to print these on small QR codes and also print them out and put them in a safety deposit box where, in the worst case, you might want to reenter this by hand. I'm reminded, for example, that if somebody had data on an MFM hard drive today, they'd be hard pressed to find an MFM controller and an ISA bus that they can plug that controller into in order to get the data off it.

Despite the fact that we're seeing technology move forward, paper predates computers, and it may well postdate them. So that's our ultimate backup medium, and I want to make that practical to use for storing the SQRL identities because we have technology available to protect paper. I loved Bruce Schneier's famous comment, is "Write your password down and put it somewhere safe because it's better to have a password complex enough that you have to write down than one simple enough to remember because people know how to protect pieces of paper." So that's all done. The spec is finished. I will implement that next and then continue moving forward.

And I did have another really neat piece of SpinRite mail that I found this morning when I was going through our Q&A questions, written by someone who just identified himself by his first name, Matt. He sent it on Sunday the 25th, so two days ago, from Waterloo, Ontario. The subject was "SpinRite Saves the Day." And he said: "Hi, Steve. I'm a fourth-year computer engineering student at the University of Waterloo, and SpinRite recently saved my team and me hundreds of hours of work. During fourth year, we have to come up with a design project that showcases what we have learned throughout our degree. My team had worked for over a year on our project and had most of it stored on one member's Lenovo laptop. Three days before the project was due..."

Leo: Seems like a bad idea.

Steve: Three days before the project - well, to their credit, they had a backup. But he says: "Three days before the project was due, his computer would no longer boot. We hadn't backed up the project in over a week." But you can imagine, with them being three days away from due, and students being who students are, a huge amount of work probably occurred between that last backup and the time that suddenly this Lenovo laptop would no longer boot. So he says: "So it was critical that we got our data back. Since the system wouldn't boot, we tried putting the hard drive in an external enclosure to recover just its data. But the drive wouldn't mount on any of our systems.

Desperate, I remembered that I had purchased a copy of SpinRite a few years back and had it burned on a CD at my apartment. I raced home to get the CD and popped it into the laptop. Sixteen hours later, SpinRite had fixed and recovered the data in more than 50 bad sectors, and we were able to pull the data we needed from the drive. Thanks for your hard work and for the excellent podcast. Matt." And, Matt, thank you for the story.

Leo: Did they say what the grade was?

Steve: Haven't heard. But I'll keep an eye out.

Leo: I'd be curious.

Steve: Yeah. And then I'll just wrap by saying that I'm continuing to get feedback. I have a freshly shaved puss here, courtesy of Harry's. Someone named Brandon who tweets as @BScottX said: "Reposting my @harrys recommendation. Best shave ever and better prices. Glad to see they're now sponsoring Security Now! with @SGgrc on @TWiT." And I'll just mention that others have reported similar amazement at the quality of their shave. And I've heard from a bunch of people who are ordering. And in every case I've said I want to hear back. Either way, if you're not impressed, if you are, just let me know because I'm...

Leo: You've got to stop doing ads without people paying you because that's - are you ready, Steve? We've got questions for you.

Steve: Yeah, you know, I'm self-conscious about talking at Harry's, so we ought to mention that we do have a Security Now! promo code there.

Leo: No, you're not allowed to use that. There's no Harry's ad right now.

Steve: Oh.

Leo: Steve, you undermine my ability to charge Harry's if you give them free ads and promo codes. You see what I'm saying?

Steve: I figured you got credit for it no matter what.

Leo: But they didn't pay for it. Yeah, I get credit for it. That's nice.

Steve: But then they know their advertising...

Leo: All right, go ahead. What's the promo code? I'll explain how advertising works a little later, off the air.

Steve: Okay.

Leo: What's the promo code?

Steve: It's Security Now!.

Leo: It's not, it's TWIT5. But go ahead. Isn't it? Is it Security Now!? Does that work? All right. It may not work. That's the problem, Steve.

Steve: Oh, that's not good.

Leo: I think it's TWIT5. But I'll have to go through. See, when they don't buy ads in the show...

Steve: Well, they bought one last week.

Leo: I can't - he's irrepressible, folks. I can't stop him. If he likes a product, he's going to talk about it. You know what, the way to find out, if you go to TWiT - I'll do it right now for you, save you some time. If you go to the website, TWiT.tv, there's a sponsor's page, and you can see what the current codes are for any given sponsor. And it might be Security Now!. Let me just check. Let's see here. Sponsors [humming] Harry's [humming] oops, that went to the site. Didn't want to do that. Let's go back. Yeah, the offer code TWIT5 will save you $5 off your first order.

Steve: Ah.

Leo: I don't know what Security Now! will do. Go ahead and try it. If it works - it might work. But this is the one I think that's currently on. You know, I'm going to go buy some stuff from Harry's and see if Security Now! works. And then, while I'm doing that, I'm going to ask you a question. Are you ready?

Steve: I am.

Leo: Herb Flores, he tweeted at you. His Twitter handle is @HerbFloresDNA, so apparently it's not him, but it's his DNA tweeting at you: Listening to Episode 456 made me wonder, how do you juggle so many projects? Could you share your methodology on project management, Steve?

Steve: Okay. So this sort of tickled me when I saw it because I would argue that I juggle projects badly. I am...

Leo: I've just checked. Security Now! does work. Go ahead and use that one.

Steve: Yay.

Leo: Yay.

Steve: Okay, cool. Thank you. I'm glad we didn't have any fall in the gutter, so...

Leo: Nobody lost is the result.

Steve: Okay. So I am obsessively monotasking. And it's just the way I operate. It's a funny characteristic of my personality. I'm unable to talk to anybody who doesn't appear to be paying attention. Because I am unable to listen to somebody I'm not paying attention to, I just assume nobody else is, either. And I'm always happy to wait until I have their attention, then I'll talk to them. But if they're busy doing something else, that's not a problem. I just - but I cannot speak. And so I've just sort of noticed that about myself.

The people who have followed the work I do in the newsgroup are pretty much acquainted with the way I operate. And that is, I am working on SpinRite 6.1, and something happens. And it's like, oh, no, crap. And as it is, I finished the phase of work I was on on SpinRite before I switched to SQRL. And now I'm working on SQRL. And then, oh, no, something happened called Heartbleed, and that brought up the whole revocation thing. And so I stopped working on SQRL, spent a couple weeks on revocation, which seemed really important to me at the time, and then resumed work on SQRL, essentially popping the stack. And I will pop the stack again once SQRL is up and running and return to SpinRite 6.1.

I dislike doing that because I call it the "switching cost." There's a substantial cost to me switching projects, just getting your head in the game. I mean, I've lost a lot of the context that was completely current when I was deep into 6.1. It'll come back. I mean, I created it from nothing initially, so I can get that context back. But, you know, so I resist distraction. I try to focus on things that are important. But I'm actually not juggling many projects, or at least not at the same time. Yeah, people sometimes say, hey, how's SpinRite 6.1 coming? It's like, well, it's not. I mean, I'm not doing SpinRite and SQRL and certificate revocation. I'm only doing one thing at a time because it's just the way I operate. I mean, I don't know how anybody can do multiple things at once.

And also I become the thing I'm working on. I mean, it's on my mind when I'm in the car. It's on my mind when I go to sleep, when I wake up in the morning. I mean, I'm working on this thing all the time. So that's the way I want to be. I want those kinds of projects that I can saturate myself with. But it's only got to be one thing at a time. So that's my mode is obsessive monotasking.

Leo: Question from Andy Olson, also on the Twitter, Average Andy, @AvgAndy on the Twitter: ICYMI. I don't know what that means. It's an acronym of some kind.

Steve: Yeah, don't recognize it.

Leo: My request: Could you make the entire Security Now! archive available via BitTorrent Sync?

Steve: Now, this represents a request that we've been getting a lot more often. And so I just wanted to acknowledge that there's a problem for me. And when we were talking with Brett, I recognized that I'm a content provider of this archive of Security Now!

podcasts. And I pay for bandwidth on, you know, very expensive bandwidth. I'm in a Level 3 datacenter, so I'm a Tier 1 connection to the Internet. And I don't know exactly. It's maybe - it's thousands of dollars a month.

And the way you pay when you're in a datacenter is a so-called 95/5 rule, where you agree, you have a certain bandwidth cap, and that's what you - and so that sort of sets a minimum, which you pay every month. And as long as the 95th percentile of your usage is within that cap, you're okay. So it allows me to, like, have bandwidth spikes. As long as they are spiking above that, as long as sort of the 95th percentile, when all of the different bandwidth chunks on five-minute segments for the month sorted end up being less than that, I'm okay.

The problem is, if I took all of this growing archive of nine-plus years of podcasts, it's very easy for someone to say, oh, I'd like a copy of that, and to press a button, and for GRC to serve that to this user. And it's not that I don't want people to have the archived audio. It's that they may never get around to listen to it. I mean, I've had to serve the bandwidth, but they may not have needed it or even end up listening. If I make it that available, it's easy to ask for, and just seems very inefficient. Also they could never listen to it in anything like the period of time they could download it.

And that's the other point is that bandwidth which is spread fits within this cap, this 95/5 bandwidth deal, which is how all datacenters operate. And so it makes much more sense for people to download them in small pieces and listen to them and then download some more. That spreads it out so everyone has access to it, and it fits within the cap. And people have said, oh, well, then, make it a torrent. Well, okay, but then it's not reliably hosted. It still has to get hosted somewhere. And if it's not available from other people who are up and running and providing alternative sources in the torrent, then it falls back to us, and we're back in the same position, or it's unreliable. And I don't want to offer unreliable, kind of flaky torrents. So anyway, what I may do at some point is create a channel which is bandwidth-limited so that I could stream a large content out in a way where, for example, it would use quality of service, and it would be at the bottom...

Leo: Hold on. Can I just say that we offer every episode of Security Now! for free at TWiT.tv/sn. Every episode is there.

Steve: But they want to click one thing.

Leo: Oh, and download it all, all of them at once.

Steve: Yes.

Leo: Well, we can do that, if you want. I don't think there's a huge demand for, what is it, 457 episodes?

Steve: I do, I get this all the time.

Leo: Somebody says I want to click one button and download all 457 episodes?

Steve: They want the archive.

Leo: That's, like, a lot of data.

Steve: Exactly my point, yeah.

Leo: No, we'll do it. If that's really - if there's the demand for it, we could do it. But you can do it, you could write a script that would download them one by one, if you wanted.

Steve: Right. And I see those dialogues go by. People, like, they use curl and all kinds of different scripting things. And, I mean, there really is an interest in obtaining the archive.

Leo: Well, and BitTorrent Sync wouldn't be the way to do it. I think this guy means BitTorrent, is what he's thinking, would somebody seed. And if somebody wants to do that, there's nothing to stop you from doing that. If you have all the episodes, zip them up and seed that as a BitTorrent seed. We'll be glad to put the BitTorrent link to that, if you want. I mean, that's the other way to do it. That would cost nobody any bandwidth.

Steve: Right.

Leo: BitTorrent Sync's not the way to do it.

Steve: Right.

Leo: I wonder how many people really want all 457 episodes.

Steve: I'm seeing it more and more. I guess, as we create an archive, people are realizing, wow, you know, there's stuff here. It's like, well, that's true.

Leo: All right. Hmm. Well, Andy - actually we'll extend this to anybody who's listening. If you want to make a - it's not BitTorrent Sync. That's a misunderstanding of what you want. If somebody wants to make a BitTorrent seed of every episode, all in one zip file, you certainly can do that. And we would even publicize the link. How's that? It's our license that allows it.

Steve: Yeah. I'm sorry, go ahead.

Leo: We could if, by the way, the way BitTorrent works, the more people who seed it, the better the response time is. So it would be good if we'd get, like, five people

to seed it. Or if you use BitTorrent, and you get the entire thing to keep it open and let it run and let the seed run.

Steve: Right, exactly.

Leo: I'm really curious how many people really want that whole thing. I wonder how big it is, too. That guy who did the thing, the graph...

Steve: So people should tweet to @leolaporte.

Leo: Yeah, do. I'll do that, yeah.

Steve: Yeah, because that'll give you some sense. Because I see it all the time.

Leo: If we did it in BitTorrent Sync - no, that's not how it...

Steve: No, you're right, you're right, no. Sync is for little private networks.

Leo: Yeah.

Steve: Yeah. It needs to be BitTorrented if it were going to make sense.

Leo: Right, right. I mean, I guess you could do it with BT Sync, but it would be weird. Will in North Texas wonders about your use of www.steve.com. I'm not sure, he says, I'm not - oh, by the way, ICYMI? In Case You Missed It.

Steve: Ah. I did, as a matter of fact. And I even missed the in case you missed.

Leo: In case you missed it. That's the first time I've seen that, although John knew it. ICYMI. Question 3, Will in North Texas. I understood your comment about no top level domains called "steve." I'm NOT sure I understood. There is a steve.com.

Steve: Yes, there is. And, boy, do I wish I had that.

Leo: Of course there is.

Steve: But I don't. Yeah, of course there is.

Leo: Of course there is.

Steve: So several people were confused, which is why this bubbled up to Q&A-worthy. What I use is not www.steve.com, but www.steve. So the .com is the top-level domain, or in my case www.steve, steve is the top-level domain. So the root or top-level domain are .com, .gov, .edu, .net, and .org and so forth. And so within my own network here in my office, where I work in code, my DNS server has entries for www.steve and just .steve. And basically it emulates the structure of GRC so I'm able to use code which, for example, bounces people from GRC.com to www.GRC.com, verify that's working by having my own little weird "steve" network. And so that's what that's about. So, sorry if I confused anybody. But I actually did mean top-level domain is Steve, as opposed to second-level.

Leo: And how do you use this? With Hamachi or what? Huh? It's local host. It's a local host.

Steve: Well, yeah. You could use the hosts file.

Leo: Right.

Steve: I run a BIND DNS server here, so I actually have a - what's the term in BIND, or in DNS? It's not a region. It's got a whole jargon.

Leo: Here's the point. If you run your own DNS server, you can do anything you damn well want to.

Steve: Exactly.

Leo: Include linking to "steve." By the way, you don't have to do www, you could just type "steve."

Steve: Oh, and I do. And then it bounces me over to www.

Leo: And, thanks to the chatroom, here is Seth Leedy's GRC Security Now! Podcast Download Script [techblog.sethleedy.name/?p=24172]. It's a bash script, if you've got access to Linux or Macintosh. It can look at the episodes already downloaded, download the next one. You can specify all or a range. You could specify whether you get the PDF or HTML for the transcript. You've got every...

Steve: Boy, that's what's been going on. I've been seeing people using that because I look at my bandwidth, and I go, okay, this strange. This is a little odd.

Leo: I would suggest you modify it to point to Cachefly so that it doesn't cost Steve any money. Let it cost TWiT money. But you'd have to modify the script. And then somebody's saying, you know what, you can use BT Sync as a kind of a peer-to-peer drop box for people. So I guess what I should probably do, maybe I'll make this a project for next week, is download all the episodes.

Steve: Oh, wow, and put them in a folder.

Leo: Put them on my machine. Put them in a folder. What would I share? What BitTorrent would I share my - that long number?

Steve: Yeah, you'd use that crazy 256-bit random string as the, you know, in very much the same way that bitcoin uses that as an address that you send things to. You would publish that and say, hey, you know, connect to this, and there's all your - there's your files.

Leo: Apparently that's what Dvorak and Curry do for No Agenda. They have a BT Sync distribution.

Steve: No kidding.

Leo: Well, you know. They're cheap.

Steve: And where does Dvorak - Dvorak's not paying for bandwidth. I wonder who sources that?

Leo: Oh, well, that's the beauty of BT Sync. It doesn't cost any, you know, the bandwidth's got to be minimal; right? And they are using a QR code to share that key, as well as the big long key.

Steve: Right, look at that nightmare.

Leo: Yeah. So this is good. So there's a shared archive folder. And that's 54 gigs. So that's the key to this is that, by doing this, I could update it. As a new show, I could just put the new show in it and so forth. And it would automatically be updated; right?

Steve: Yeah.

Leo: Wow.

Steve: Oh, and it would automatically sync to people's drives. It would send it out to everybody who wanted all...

Leo: All seven of you that want every episode, just automatically stay up to date. Seth Leedy's GRC Security Now! Podcast Download Script is at SethLeedy.name. Ready to move on to the next...

Steve: Oh, more than.

Leo: Steve.com? Kelly Shipp in Conway, Arkansas wonders what the heck's going on with port 80 and 443: Steve, I recently set up hosting at Rackspace and created a site with an SSL certificate from your favorite vendor, DigiCert. Do you have an offer code for them, Steve? Actually, you know what, they approached us about advertising. They said...

Steve: I wouldn't be surprised.

Leo: Yeah, Steve loves us so much.

Steve: They know I'm a fanboy.

Leo: See, here's the problem. When you give them free ads, they don't buy ads. It's like, we don't need to buy an ad. Steve is just going to plug us.

Steve: I'm not going to tell you who my favorite...

Leo: Exactly. I'm all for you telling us your favorite everything, from razorblades to certificate authorities.

Steve: Science fiction.

Leo: And so science fiction, absolutely.

Steve: Oh, and speaking of which, just a reminder that, finally, "Halt and Catch Fire" is this Sunday. So anyone who's been...

Leo: I'm seeing mixed comments on it now. I haven't seen it.

Steve: Yeah. I saw, I watched the first five minutes of their premiere episode. I kind of, I don't know.

Leo: It does look like it's Compaq because at one point they say we're going to reverse-engineer the IBM PC. So...

Steve: Yeah.

Leo: Yeah. Kelly Shipp, Conway, Arkansas. So remember, set up Rackspace, DigiCert. After I set-up an initial test page, I discovered, even under HTTPS, the secure HTTP, the server was responding via port 80, not 443. In Firefox, the lock in the address bar is locked, as hoped, so all seems well from the client side. I'm still - I'm concerned the server is saying it's communicating via port 80?

What's going on there? Oh, there's more.

I contacted Rackspace support, and they said: "Connections to our network are over 443, but the traffic passed inside to the Apache/PHP nodes is managed with port 80. After any necessary processes are complete, that data is passed back to the load balancer and transmitted over port 443." This tells me that traffic inside their network is insecure. What are your thoughts on this? I've never known a host to screw with a port number like this. Thanks, Kelly.

Steve: That is exactly their architecture.

Leo: But that's a shared server architecture; right? Or even a dedicated server?

Steve: Actually, this is a frontend SSL load balancer.

Leo: Right.

Steve: So this load balancer machine is the one that is receiving and terminating all of the SSL connections. It has the certificate that Kelly loaded into it there. And so what happens is when someone connects with it, it does the three-way handshake. The user than sends their query over SSL to it. It turns around and then initiates a standard TCP connection to the server on the backend, which is just port 80. So none of those servers have SSL or certificates or any of that. That's all handled by - that's probably an SSL accelerator. It's probably got hardware SSL to allow it to handle a huge volume of connections, much more than software in the server would be able to handle. And then all the servers just see port 80.

But Kelly's right. What this technically means is there are wires inside Rackspace where the encryption is stripped off as it goes between the load balancer and the server. Now, is that a concern? Well, I guess it's good to know from a security standpoint that that's the architecture. You're already trusting Rackspace...

Leo: Yeah, I mean, they have access to those wires. They have access to your server itself; right?

Steve: Precisely. So they could certainly run something in the server, if that's what they wanted to do, in order to spy on you. You might argue, well, this makes it a lot easier, but that's not why they've done it. They've done it because they want a very high-speed hardware SSL accelerator, which also functions as a load balancer in order to distribute traffic, and then all the certificates go there. And then you just have much simpler to set up and deploy servers on the backside where the security is handled for them. There are many things you could not do with that architecture, that is, GRC could never operate that way because I'm intimately involved in all kinds of aspects of the specifics for the services that GRC offers, which are security related, check your fingerprints on your certificates and all that kind of stuff. But for a website that wants to be able to offer security, this does the job, and this is just the architecture that Rackspace chose.

Leo: So if you're an ecommerce site, for instance, you wouldn't have to...

Steve: Yeah, you're okay.

Leo: I'm sure they all work this way; don't they? I mean, I'm sure Amazon, once the SSL traffic gets to the front of Amazon, as soon as it's inside the...

Steve: Right. The only difference there is that everyone behind their accelerator...

Leo: Works for Amazon, right.

Steve: ...works for Amazon, exactly, instead of being a multihosted environment.

Leo: Presume you can trust Rackspace. And if you couldn't, you have deeper trouble anyway because they have keys to the server, as well. They can pull the hard drive if they want and examine it and take all the data off of it and that kind of thing.

Robert Van Etta in Guam, United States of America, worries about the "ghost in the machine": Allow me to dip into the paranoid side of things, he says, and perhaps you could provide some calibration. I recently discovered my tablet uses a single chip, the BCM - Broadcom - 4330, to handle all wireless functions. It also has an integrated ARM processor with onboard memory. This is in addition to the tablet's CPU and RAM. I am concerned that nefarious firmware on the wireless chip could potentially allow it to function as a backdoor to my system. Unfortunately, closed source firmware makes it difficult to know for sure what it is or isn't going on. What do you think? Is it time for me to worry or remove my tinfoil hat?

Steve: Or maybe add another layer. He's absolutely right. This is the architecture of modern systems. No longer are they singular processor solutions. We've been talking about the security of the iPhone, where it's got a fingerprint processor and a camera processor and a security processor and a main processor. I mean, now we've got little networks of independent processors running.

Leo: It was worse before. If you...

Steve: Yeah.

Leo: I mean, the only thing systems on a chip do is they get them closer together. An early IBM PC, you had different chips doing all different things; right? You serial chip...

Steve: All through the bus.

Leo: Yeah. It was all over the place. Your modem might not even have been in the computer.

Steve: Yeah. We also have his whole issue of the baseband, the so-called "baseband."

Leo: Yeah, we talked about that, yeah.

Steve: Yeah, which is sort of what this is, where it's a processor, typically from Broadcom, that's, like, doing all of the cellular stuff. And, unfortunately, it's sort of a black box that the various phone providers just stick in.

Leo: And it's crappy.

Steve: And it does...

Leo: It's crappy software.

Steve: Exactly, exactly. Old and potentially buggy and crappy. And it's not anything like this beautiful security architecture that Apple designed for iOS.

Leo: But it's the way it's always been. This is not anything new.

Steve: Yeah. So I think that there are better things to worry about, I guess is the way to put it. It's like, yeah, I mean, it could be bad. But you really, if you're going to use any of this technology, you've got to trust someone.

Leo: Yeah, I think people don't understand that, unless you go in a cabin and seal the doors, there's always somebody else.

Steve: And read paper books.

Leo: Yeah. No electricity. Athol Wilson - I don't know, am I saying that right? Athol? Athol Wilson.

Steve: Well, you want to make sure you pronounce the "T."

Leo: Athol Wilson in Auckland, New Zealand further pondering questions of entropy, our issue, our topic of last week: Steve, I just had the thought that with many still convinced that a collision is not impossible, and you mentioning that not all of the original 512 bits were being used to generate keys, if additional nonrandom bits were included that contained, say, 32 bits of the current time in seconds, about 130 years before it repeats, would this not restrict a collision to just those generated in exactly that second? As the rest of the bits are still truly random, would the additional portion of nonrandom bits degrade the use or security of the generated key, or perhaps enhance it? He's saying add a timestamp.

Steve: Yeah. And it's really an interesting thought problem. And it reduces the security. The reason that happens is that we've got 32 bits that are not going to be changing very much. And that's true to the point that it takes 130 years for all possible combinations of them to come up. Yet the lifetime of key generating with a given version of SQRL, what, maybe a decade, maybe 20 years? So the point is that many more combinations would never be used that could have been used to reduce collision probability. And essentially what this means is, if we had those 32 bits, it is far better to make them as random as possible so that we're using all of them, all of the time, then sort of reserving nine-tenths for a period of time, after which SQRL was probably even in use. So, yes, you cannot get better than allocate as many bits as you feel you need, but nothing is better than random.

Leo: I love that. That is a great thought problem because you're saying, well, I am so concerned about the purely theoretical and highly unlikely possibility of collision that I want to add this timestamp. But in order to do that, I have to reduce the possible options. Admittedly, the timestamp then keeps it from having a collision but once every 130 years. But as it turns out, you're cutting so much entropy out of it that you're still better off allowing the possibility of a collision. The collision thing bothers people, though, doesn't it.

Steve: It does. It's just - and this is why one of our recurring themes is how bad humans are about probability.

Leo: We don't get it.

Steve: I mean, it's like, okay, yes, so it's 10^45 times more likely that we're going to be killed by a meteor strike in the next second. But it could happen.

Leo: It could happen.

Steve: You know? It could happen.

Leo: It could happen.

Steve: It's like, okay, yeah.

Leo: So what you're saying, though, I want to make this clear, is this an opinion that it would be better to have the entropy than to have the timestamp?

Steve: No.

Leo: No.

Steve: Absolutely provable.

Leo: Provable.

Steve: The idea would be we would - say we had 256 bits. Athol is suggesting we take 32 off the top. See, we have to take them from somewhere. So we pull 32 down from the...

Leo: Or even if you didn't, even if you didn't, it would be the question is would it be better to use any additional 32 bits for a timestamp or randomness?

Steve: Random is the answer.

Leo: It's always going to be random is better.

Steve: Always, yes.

Leo: Always.

Steve: Absolutely always.

Leo: I love that. And we still don't get it. But Steve, there could be a collision.

Steve: Okay. The only time it would not be better is if we considered all collisions of all keys generated in 130 years.

Leo: Ah. The birthday problem.

Steve: Because then we would have used all 32 bits for the generation of active keys. But it would take 130 years in order to use all 32 bits. And then looking at all the collisions of all the keys in 130 years would be the same as if it was random from the beginning.

Leo: But the likelihood of you having a collision is still...

Steve: Yes. Clearly better if we're using all the bits, all the time.

Leo: Love that. Love that.

Steve: Yeah. Yeah.

Leo: That is math. What a concept. Jason in Winnipeg. He wonders about a SQRL entropy interception possibility: Steve, on the most recent Episode 15, I'm sorry, 456 of Security Now!, you mention there's no way for an attacker to intercept or modify any instruction that your program executes in its own process space, in particular the RdRand instruction. Are you sure about that, Mr. Gibson? If we're already supposing that an attacker has the means to intercept calls between the process and the OS, then we necessarily assume the attacker has root privileges on the machine. That means they are also able to insert their own kernel modules into the system.

While the RdRand instruction only returns random numbers to registers, well, of course it's impossible for a program to predict when the OS scheduler decides that CPU time is up and gives another process a chance to run. During that time, all of the general purpose registers, which is where the RdRand stores its return value, get swapped out of registers and stored into kernel memory. Therefore, couldn't a hostile kernel module be constantly scanning kernel memory for SQRL's process control block and intercept or modify the value returned - this is a determined attacker - and intercept or modify the return value, returned from RdRand, by changing the saved contents of the register?

That said, if the above is possible, then the rogue kernel module could also modify the final output of the SHA-512 hash, or even SQRL's code itself. It seems insane to talk about security in the context of an attacker having root access to your machine, but isn't that required in order for an attacker to be able to intercept any of SQRL's OS calls in the first place?

Steve: So this was a great question. And it reflects something that I didn't expressly address last week. And that is that it's useful to do the best job we can, while recognizing that, bottom line, we're software running in a computer. And we're only as secure as the

boundaries and limitations that the hosting operating system provides. Now, if you assume that an attacker has full root admin privileges, which, you know, there are many attacks which are effective that don't have that. So, for example, the famous return-based attacks, where you jump into kernel code to get some instructions executed in kernel space and then return to you - ROP, Return-Oriented Programming, it's called - that's sort of a limited case.

It is true that, if an attacker had complete root privilege, then, for example, they could set a hardware breakpoint because the Intel architecture - and in fact all modern chip architectures support hardware breakpoints to allow debugging. You could insert a hardware execution breakpoint after the RdRand instruction in order to obtain its data. Or, as he points out, stick it after the SHA-512 hash. Or, the point is, if you have that level of access, then what we're trying to do is impossible. We're trying to have secure software where an attacker has absolute control over the program. And it's not possible.

Leo: Good luck.

Steve: That's why we have so-called HSM, so Hardware Security Modules. It's why one of the modes for using SQRL is to use a cell phone, which, unfortunately, that's also a likely victim. There are people in the newsgroup who have considered, and I'm not sure where they are on this, they may be well along, building a little SQRL Authenticator, which is just a standalone piece of hardware with the SQRL crypto technology in it, which is not infectable because it's not wired into a common operating system platform and wireless everything. So that's sort of where you have to go if you want absolute security in the face of an absolutely capable attacker. So recognize that I'm able to make something freely downloadable, which is just software, which is going to be very secure. But it certainly assumes some integrity of a security perimeter around your programs.

On the other hand, everything we do does. When we enter our credit card number into the form on a browser, we're making that assumption, that nothing is there in our computer, watching our credit card. Unfortunately, sometimes there is a keystroke logger that is doing that. SQRL is better in that it doesn't give keystroke loggers anything to get. And what's also interesting is that in the very, very, very worst case, and that's one thing that SQRL handles, if an attacker got everything, absolutely everything you have, there is this other notion of what SQRL keeps offline, which is the rescue code, which allows you to take back a stolen identity from an attacker. And that's because it's offline. It's not available in the software to be attacked. So we actually even have that covered, as well.

Leo: That's reassuring. I like that.

Steve: Yes, yes.

Leo: I think sometimes people take TNO a little too far.

Steve: Well, it's, yeah, there are limitations because we're operating in an operating system with a lot of things going on. And the benefit is this can all be free. The liability is that it's not as safe as if it were hardware. And the good news is SQRL does provide a backup of last resort with the so-called "rescue code" that allows you to, if your identity

got stolen, to foreclose that and take your identity back.

Leo: That seems more than adequate to me.

Steve: Oh, yeah. That's why I'm taking all the time to do this.

Leo: I actually like that. Google does that. You know, it's very important that you give them a phone number so that, if all else fails, you can have a reset sent to that phone number. Unless the attacker has everything, including your phone, you could take it back. You say, no, I'm changing the password. Whoever got this and changed it, I'm going to change it back.

Ken Clarke, Dartmouth, Nova Scotia notes eBay has reduced password security in response to its data breach: Steve, I know you mentioned the data breach at eBay. What you may not know is one of their responses is to force users to use shorter passwords. We talked a little bit about this. Yes, I said shorter, in my case a lot shorter. Their system, for a decade or so, at least for the decade I've been a member, has supported a password length of up to 64 characters. However, after receiving an email announcing the breach and asking me to change my password, I went to the site - typed in the URL, not clicking a link - and was forced to - which, by the way, they do provide you a link in the email, bad idea - and was forced to change it to a maximum length of 20 characters. Even though the HTML for the input field supported the full 64 characters - it uses the attribute maxlength="64" - the response to my attempt at entering a longer password was, and I quote, "Your password cannot be longer than 20 characters." Man, if ever we needed SQRL, it's now. Keep up the great work.

P.S.: Calomel gives eBay's SSL certificate a failing grade, as well. I'm slowly reaching the conclusion that I don't want to leave important information in online databases anymore, when large entities such as this don't understand basic security. Of course, eBay owns PayPal, which makes this even more concerning.

Steve: Yeah. Yeah. So anyway, we discussed this before, as you said. This was the post I knew I was sort of stepping on it because, for whatever reason, eBay made this decision. I think probably...

Leo: Is there any technical - it is possible that doing this made it more secure in some way that I can't possibly understand?

Steve: The only thing I could think is it is a technical support issue, or someone just made an arbitrary decision. Oh, 20 characters is enough. We used to support 64 back when the geeks were running things.

Leo: Why would you go backwards? That's what I don't get.

Steve: Yeah. And funny, too, because even their input field, as he mentions, still says maxlength="64". So the HTML form that you submit it will send it all to eBay. Then eBay

looks at it and says, whoa, okay, no.

Leo: Yeah, too much.

Steve: Yeah.

Leo: Geez. Weird.

Steve: Yeah. But my point was they do support upper and lowercase, special characters, and just absolute gibberish. And 20 characters of a 96-character character set is a huge amount of entropy. I mean, you can drop it into the Password Haystack and see how many combinations there are. That's really all the security you need. I mean, they will get their database hacked again before anyone breaks one of those.

Leo: Yeah. Wow. So that's good to know. In fact, you should be more worried when they say "no special characters" than when they have an arbitrarily short limit.

Steve: True.

Leo: Unless the limit's eight.

Steve: Yeah. Yeah. And it's weird, too. I think their lower limit, is it eight or six?

Leo: I don't know. Six sounds right.

Steve: For some reason, I think I saw someone said six. It's like, whoa, that is a little short. I mean, if you want to do anything, bring that up to 10. But then it's like, oh, my favorite password is only...

Leo: I can't use "monkey."

Steve: Yeah.

Leo: "Monkey," want to use "monkey." Six, huh? Michael "Waddy" Waddell in Chicago, Illinois proposes a way in which Shubham's - is that how to pronounce it? Shubham? Shubham?

Steve: Yeah, from last week.

Leo: Shubham's two-factor bypass is a practical attack. Oh, that's the one we were talking about last week, yeah. During Episode 456, you discussed Shubham Shah's two-factor bypass. It was dismissed as impractical because you'd need to already have the password in order to use this attack. Now, here's why I can see this being exploited on a larger scale, because of the way that most sites implement two-factor authentication: For every site I've used two-factor with, if you enter an invalid password, you get an error message. But if you enter a valid password, then you get the second-factor prompt. Yeah, that's right. This effectively gives an attacker feedback on whether or not they've successfully guessed the victim's password.

If the victim's using a simple password because they feel that two-factor's protecting them, their password could be compromised by a dictionary attack. A botnet could be used to brute-force a large number of accounts, then send back the username and password for any accounts that offer up the second factor prompt. Hackers could then do reconnaissance to obtain the cell phone numbers of those targeted accounts in order to use Shubham's attack. I can see this being effective because of the user belief that two-factor allows them to use a weaker password - hmm - than they would use if they didn't have...

Steve: That's a good - it's a good point.

Leo: Yeah, it's a good point, yeah. A simple fix for this would be to request the second factor regardless of whether the password is correct, in order to eliminate the feedback that the attacker gets from the current implementation of two-factor.

Steve: And you know why they don't?

Leo: Why?

Steve: It would create a huge denial-of-service attack.

Leo: Oh, yeah.

Steve: What that would mean is that...

Leo: Oh, yeah, you're right.

Steve: Yup.

Leo: Holy cow.

Steve: Uh-huh.

Leo: Just enter wrong passwords in mass quantities. Hoh, what a mess.

Steve: Yes, it would just be a catastrophe. So, I mean...

Leo: It's a good point.

Steve: So he's absolutely right. Huh?

Leo: It's a very good point.

Steve: Yeah. Yeah, he's absolutely right that this does provide some feedback. And we've often talked about how you should never say, oh, your username is wrong, or your password is wrong. You should absolutely wait until you have both and then say something is wrong, but don't give the attacker - give the attacker as little information as possible so they don't know how to navigate. But exactly as we said, if the two-factor authentication was triggered with every submission, oh, my god, that would just be the end of the world.

Leo: Imagine the number of text messages going out over the network. Hey, is this, could it be, it is, the last one. Man, Steve, you're good.

Steve: It's a team effort, Leo.

Leo: Yes, it is.

Steve: Team effort.

Leo: It's a team effort. Steve Rea, Rochester, New York wonders about life after SpinRite: Long-time listener, love the show, blah blah blah. I hear the glowing testimonials about SpinRite saving somebody's files, but should you - oh, and, you know, I get this a lot.

Steve: Yeah.

Leo: And I'm glad that he asked. Should you trust a drive that has had failure that SpinRite's fixed? I would think that would be an indicator to get a new drive as soon as possible. If SpinRite keeps fixing problems, I would think you would want to stop using the drive. Any thoughts? Anxiously awaiting the Mac-compatible version of SpinRite. I'm a few months behind in the podcasts, but I'll keep listening. Damn you, Leo, for having too many good shows to listen to. That's a problem I like having.

Steve: So it is absolutely the case that there are failures of a drive to read sectors where there is nothing wrong with the drive. If when a drive is writing, you vibrate the drive, or you give it a little tweak, like a tap on it, a vibration, that will knock the head off track. Nothing wrong with the drive. Nothing wrong with the sectors. But those sectors and probably the adjacent group will no longer be readable because densities are so high, drives have become incredibly sensitive to vibration.

I remember talking a couple years ago about someone who noticed - well, in fact, remember the guy who was shouting at his drives? He was shouting at his server, and like the bandwidth of the server dropped when he was shouting at it because the drives were having to do retries in order to go back and try to get data that was even uncorrectable the first time. If that happens when you're writing, you will write off track and wipe out the neighborhood. SpinRite can come along and fix that kind of problem. But never is there a problem with the drive. It's just the environment. It's the nature of the technology.

That said, we talked about this Lenovo laptop at the top of the show, where SpinRite recovered over 50 sectors. When I hear that, and they're, like, finally it wouldn't boot, and I think, wow, if they had just run SpinRite a week before, like run SpinRite after you do the backup. They were backing it up, but they weren't running SpinRite. SpinRite would have fixed those latent problems before they became crucial and, essentially, by rewriting the data on the tracks where it's supposed to be, prevent this from becoming a problem.

So in a laptop, you know, laptops get all kinds of abuse. There may have been, like, physical head crashes because the heads are very close to the platter. People tend to bounce their laptops around while the drives are still spinning. There you're causing some mechanical problems. So my point is there isn't a single pat answer to this question. The best thing to do is watch the SMART screen. There's normally three or four, depending upon how many parameters the drive publishes, graph bars, or also called bar graphs, graphical bars on the screen. And people have just in the last week been tweeting me pictures of theirs where the cyan color is pushed down, and there's red dots showing. And that's not good. That's the drive itself saying, while I am being exercised by SpinRite, I'm reducing my own health readings which I'm sending out to the world. So that's an indication, ooh, you know, this drive is telling you it's having trouble meeting SpinRite's demands.

And it's because SpinRite is putting the drive under load that then, during that period of time, the SMART parameters matter. They really don't mean much if the drive isn't doing much work because they sort of tend to be self-healing and recovering. They'll sort of creep back up if it was doing something. SpinRite is able to see it and display it. Anyway, there isn't a simple answer. Noncritical problems can occur which SpinRite can fix, and the drive is as good to use afterwards as it was before. Or they can certainly be more of a concern. I would say maybe lower your trust in the drive a little bit, if SpinRite seems to be coming to its rescue all the time, and back up more often.

Leo: Steve, we have come to the end of a fabulous program. Really interesting stuff with Brett Glass at the beginning. I'm glad we could do 10 questions, the news. I don't know how you do it.

Steve: Some free advertising.

Leo: You understand that just because they use - we don't do what is called "cost per acquisition" ads. A lot of times people assume, oh, well, every time you mention this offer code, TWiT gets a buck. We don't do that kind of ads. So just because you...

Steve: Ah.

Leo: Yeah, that's why I thought. I thought you might have thought that. There's no revenue at all in somebody using your offer code. There's goodwill. I love that.

Steve: And are they an ongoing advertiser with the network?

Leo: Yeah.

Steve: Okay. But just not with my podcast.

Leo: Well, they come and go, as all - nobody's always on any particular show.

Steve: Right, right.

Leo: The goodwill is great. You love it. I don't have any problem with you recommending it. I just want you to understand that there's no revenue at all in your recommending it or giving an offer code. It's good for you, and I'm sure Harry's loves it.

Steve: Well, I figured that the offer code allowed them to track where the sales was coming from, so they know...

Leo: But that doesn't make - yeah.

Steve: So it would incent them to buy more advertising.

Leo: Or disincent them because why should they? They're getting...

Steve: Oh, they've already, yeah, they've already...

Leo: They got what they would get in the ad. In fact, it's better than an ad.

Steve: They got me hooked, yeah.

Leo: But at the same time, we love you, and we want to hear your recommendations. So that's not - nobody's going to say don't say what you like. It's just I think people sometimes think, and I know many of our audience thinks that, if you use an offer code, that makes us a buck or something. And for many shows, most shows, probably, most podcast networks, that's the case. But we don't do that kind of deal because I feel like it devalues the network.

Steve: It's good to know.

Leo: They pay for an ad. They pay to get the impressions. And, absolutely, if you're going to go to Harry's, use the offer code Security Now!. My only concern is I don't know if it's, you know, it comes and goes. And we try to - this is the other thing. We try and encourage our advertisers to keep all offer codes good.

Steve: Because, look, I mean, people will be listening to this a month from now.

Leo: Well, but that's the problem. They don't. So when they're tracking, I don't know why, but many advertisers expire offer codes. That's more often the case than not. So, yeah, you shouldn't; right? Don't you want the business? I think every advertiser should keep all offer codes going. Because, I mean, what's the problem? Don't you want the business? But that's not - sometimes you don't think that way. It's a very complicated thing. And you love Harry's. We love you for it. Harry's really loves you for it. Expect many blades in the mail. Actually, I don't even know if they know. I really don't. They'll probably say, oh, we're getting a lot of offer codes from Security Now!. But we don't know.

Steve: Well, our listeners know. And for what it's worth, it's been a hit.

Leo: That's what matters.

Steve: Yes, it is. We're providing value.

Leo: We're here to get you a good shave. That's what we care about. Not any of that other stuff.

Steve: That's right. We're going to give you a clean shave, baby.

Leo: That revenue, those 25 employees, that revenue stuff, that's nothing. I'm just going to have Brett Glass send me money from now on.

Steve: Yeah, good luck with that.

Leo: But I need the money, Brett. I can't do business unless Internet service providers pay me.

Steve: I was really glad we had the discussion. I thought that was very useful and...

Leo: Oh, it was great. It underscores how complicated it is.

Steve: It explains, also, that, like, the issue is where's the money going to come from?

Leo: It's very complicated.

Steve: And if we keep as like a free breakfast for the end-user or what? So, and I really think, I mean, it's going to be a tough row to hoe. But the model of the electric utility seems really to fit best, which is you're billed by your usage.

Leo: For what you use.

Steve: And if you just suck down every Netflix show ever, well, there's a cost. There's a cost to doing that.

Leo: Yeah. Yeah, that doesn't seem unreasonable. And that doesn't impact Net Neutrality. That means you pay for what you use.

Steve: No, exactly. Exactly.

Leo: I do have to think that most Internet service providers make money. He is in a very expensive kind of Internet service provider because of how he's doing it.

Steve: Well, and I stiffened a little bit when he mentioned that, like, downloading movies was very profitable. It's like, whoa, wait, hold on. That shouldn't matter.

Leo: Right.

Steve: I mean, it's not about...

Leo: Bits are bits. Bits is bits.

Steve: Right, right.

Leo: So, yeah. And so Brett is in a tough situation because he is providing what is actually a very expensive service to his customers, and apparently he can't charge them what it's worth.

Steve: And I thought it was really interesting that, to a one, the first question is, could we get Netflix? And it's like, oh.

Leo: Right. No, I understand that. But you're a wireless Internet service provider. You're buying expensive bandwidth to begin with.

Steve: In the boonies.

Leo: Yeah.

Steve: I mean, you know, he's on water towers aiming microwave dishes.

Leo: So he's not exactly a typical situation. I think Comcast makes plenty of money off their Internet service.

Steve: Right, we're not worried about...

Leo: I don't think they're going bankrupt. I think they'd like to make more. I know that.

Steve: Oh, wouldn't everybody, yeah.

Leo: Wouldn't everybody. I'd like to make more. We'd all like to make more. This show is brought to you every Tuesday, right after MacBreak Weekly, 1:00 p.m. Pacific, 4:00 p.m. Eastern time, 20:00 UTC.

Steve: Are we being affected by the...

Leo: We are not. Good news.

Steve: ...Apple event?

Leo: The Apple event's on a Monday.

Steve: Okay.

Leo: So there will be a different show ahead of time, ahead of you next Tuesday, but you will be on at the same time.

Steve: Ah, because you're moving the MacBreak over to Monday.

Leo: We're moving MacBreak to Monday, yeah.

Steve: Right.

Leo: I think iPad Today will lead into you next week. Join us live. It's great to have you. And the conversation in the chatroom is always fun and exciting. But if you can't be here live, we have on-demand for you in many ways. Soon to be BitTorrent Sync. Actually, when we started, you know, I don't know if I did it with this show, but certainly when TWiT started we used BitTorrent because I didn't have - we couldn't afford the bandwidth, so we used BitTorrent.

Steve: Ah.

Leo: Another thing that was basically cut off by broadband providers who didn't like that idea.

Steve: Yeah.

Leo: Yeah. We do this - oh, yeah, and then you can get on-demand versions. That's what I was about to say. Steve has really an interesting plan there. If you've got the bandwidth, if you're on the WISP, and you don't want to pay for a lot of bits, Steve's got 16Kb audio and transcriptions, which is as small as you can get of the show. But we also have, for those of you who are living fat and happy on the big, big, big pipe...

Steve: On the big pipe.

Leo: We've got full bandwidth audio and video at TWiT.tv/sn. If you go to GRC.com to get your copy, don't forget to visit the feedback form. That's at GRC.com/feedback for our future question-and-answer episodes. Get yourself a copy of SpinRite, the world's best hard drive, maintenance, and recovery utility. And also all the freebies and all the - there's so much stuff on your site now, it's really a fun read. Just browse around: GRC.com. We'll be back next week. Thank you, Steve.

Steve: Thanks, Leo.