Breaking SSL, PDP-8's and UltraCapacitors

Description: Steve and Leo discuss the newly discovered cracks in SSL (Secure Sockets Layer), antique PDP-8 minicomputers, and the importance of next-generation UltraCapacitors.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-177.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-177-lq.mp3

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

Leo Laporte: Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 177 for January 1, 2009: SSL, PDPs, and UltraCaps. This show is brought to you by listeners like you and your contributions. We couldn't do it without you. Thanks so much.

Happy New Year! It's 2009. Fitting the first podcast of the new year would be the podcast that never sleeps, that never rests, Steve Gibson's Security Now! Hi, Steve.

Steve Gibson: That never misses a beat. Hey, Leo. It's great to be with you.

Leo: You are now officially ahead of TWiT. You're doing very well. 177 episodes. Did you have a good holiday?

Steve: Every time I hear those Dick DeBartolo episode numbers, I just grit my teeth.

Leo: I know. In the 700s.

Steve: Yeah.

Leo: That's what happens when you do it every day. You wouldn't want to do this show every day, would you?

Steve: No, we can't do this every day.

Leo: It could be arranged. I think we'd have an audience. Well, how are you? Did you have a good Christmas?

Steve: Had a great Christmas. Had a little bit of a fall in the middle of the night on Christmas Eve, sort of somehow blackened my left eye, even though it doesn't hurt. Everything's fine. And I came down with the Christmas cold from hell. It's been really nasty. So I apologize in advance if I unconsciously sniffle or make annoying audio sounds. I will work not to do that for the next hour or so.

Leo: Well, and I'll charge Tony Wang, our brilliant editor, with cutting out...

Steve: Well, if I do a big sneeze we could cut that out.

Leo: All the snarfles will be gone.

Steve: We'll work to do that. But we have a very special episode this week. It was exactly 13 weeks ago, Episode 164, where we bumped our regularly scheduled Q&A to talk about Sockstress, which was, you know, is the Internet going to come down? Is TCP broken? All that stuff. And we said, well, no. But it's interesting, so here's what it is. So that changed the parity of the episodes, the even-and-oddness of the episodes where we do the Q&As. We're going to do that again because there's been a huge amount of news caused by a disclosure only a couple days ago of essentially an exploit in a known weakness that involves the authentication of SSL, our favorite security protocol for the Internet. Secure Socket Layer is what SSL, of course, stands for.

But even before that happened I had written to you with my intention to talk about two things that were not security related, that I just - I'm passionate about them both. I wanted to share this with our listeners. Also there's some listener involvement because there's a possibility of building a certain type of kit that I will talk about that would be available for, like, the last time ever on Earth this could happen, as a consequence of a particular chip that became available. So a bunch of stuff.

Leo: You've really got me intrigued. This is very intriguing. All right.

Steve: It's going to be a fantastic episode. We also, since we haven't been live for three weeks because we had to pre-record, we've got a whole bunch of security stuff. So I've just got tons of stuff to talk about and some really interesting things. And finally, the last thing that happened was a patent was granted on December 16, Tuesday a couple weeks ago, that discloses, as patents must, the fabrication details of a breakthrough energy storage technology...

Leo: Oh, boy.

Steve: ...which potentially obsoletes batteries.

Leo: That would be huge. It's the one breakthrough I've been kind of saying, if you could pick one, you know, this is the one because all of our portable devices are right now hobbled by the inefficiency of batteries.

Steve: Well, yes. The lifetime, the cycle length, the charging time. This technology, a so-called ultracapacitor, just makes - it makes so much sense because...

Leo: Useful for autos, as well, do you think?

Steve: Well, that's the primary target was for the whole hybrid auto market. However, it's completely scaleable. So, and it changes everything. I mean, imagine a laptop that, first of all, with the same size of battery, could give you three times the life for the same size and weight. But because this is a capacitor, when it begins to run down, you plug it in, count to five, and unplug it. It literally charges in five seconds.

Leo: I love that.

Steve: It changes everything.

Leo: It does. Oh, this is exciting.

Steve: So we've got lots to talk about.

Leo: So Steve, should we, I mean, we can't - where do we start here? We haven't talked in so long.

Steve: I know. Well, we'll exercise some discipline, although I'm so excited to talk about this...

Leo: You want to talk about your batteries.

Steve: Yeah, nonsecurity stuff. But we've got to cover a bunch of security stuff.

Leo: Well, I tell you, I saw this, I saw an image, I can't remember which magazine it was, with a Microsoft certificate saying the name of my bank, issued by, like,

Hacker.com. And I thought, what the heck is going on here?

Steve: Yes. Throughout today's episode I'll be referring to the show notes for this week. They're always accessible where they always are, which is GRC.com/securitynow. And then for Episode 177, one of the little icons there will take you to the show notes. But because I expect so many people are going to want to get to that page, I created a little SnipURL shortcut for it. So it's snipurl.com/sn177.

Leo: Oh, that makes it easy. We probably should do that for every episode.

Steve: That'll take everybody there immediately, rather than having to navigate through a couple pages. So it's snipurl.com/sn177.

Leo: All right. That's where all the details will be. Don't go there now. I don't want to spoil it.

Steve: Lots of links. Well, for example, one of the things that's there is a demo of - actually it's not there at this instant. It's on my copy. I haven't put it up on the server yet. So our live listeners will need to wait for a couple hours, and I'll get caught up as soon as we're done recording. But I will have a link to a demonstration of this fraudulent certificate where, if you set your clock back, the security researchers who created the fraudulent certificate made it expire after August of '04. So if you set your machine's clock to a certain date, during which their fraudulent certificate is valid, then you can click this link, and you will get an SSL connection from your browser to your server using an invalid certificate based on a valid root authority. So, I mean, we'll talk about what this means in detail after we cover a bunch of, well, after we get all the other security stuff out of the way we'll do that and then the other topics I want to talk about.

Leo: Big, big story, yeah.

Steve: So again, that URL is at snipurl.com/sn177. Okay. So in terms of patching there's been a lot that's happened in the last three weeks. When I turned on my Mac, my Intel-based Mac, it said, oh, we have 190MB.

Leo: 10.5.9, was it, I think?

Steve: No, we're at 6 now. 10.5.6. So there were many critical vulnerabilities that were patched. I imagine everybody who knows, I mean, who has been following along, you may want to just make sure that your Mac is up to date by telling it to run the little software update under that main menu item and give it a chance. Opera has been updated to 9.6.3 with a bunch of problems fixed. Firefox, I said last time and I'll say it again, it's time for the people who are still using v2, if v3 is available on your platform, it's time to switch to v3. V2 is going to no longer be maintained. The last version of v2 is 2.0.0.20. And that fixed a bunch of critical vulnerabilities which were also fixed in the latest version of Firefox v3, which is 3.0.5. So if you can't switch to 3 for some reason,

you do want to make sure that you're using 2.0.0.20 under Firefox 2. But no more fixes are coming down for that. So you probably do want to - it's time to move over to - it's been a year. And I'm there, and we know how reluctant I am to move. I'm just completely happy with Firefox v3.

Leo: Yes, yes, yes.

Steve: Also, Google's Chrome officially left beta. It is no longer in beta. So the Chrome browser is done. And remember we were speculating whether it would ever get out of beta because...

Leo: Most of the time Google doesn't, yeah, yeah.

Steve: Okay. But it's really nice that they got it done and made a bunch of changes.

Leo: Is it done, or is it just, I mean, it's arbitrary.

Steve: Yeah, I think they just - they decided to take it out of beta, make a v1, something or other.

Leo: Good.

Steve: Okay. Now, also since we last talked, actually it was like the afternoon of our last recording, Microsoft once again surprised us with an out-of-cycle patch. There was a zero-day exploit which they discovered that affected all versions of IE, which caused Microsoft to react very quickly. There were seven different exploits that have been identified. And at the time as many as 6,000 websites were infected with this. So this was code on those websites which was installing software in users' machines using a flaw that was not known until it was found in the wild, thus zero-day exploit. So certainly our listeners who are, I'm sure, keeping up with patches know about this. But it was substantial. And what it allowed was for malicious code to run in the context of the logged-on user.

Well, I mention that because both Sandboxie's new rights-dropping feature and the DropMyRights tool, the little utility we talked about last time, both would have prevented this. So it's a perfect example of running your browser with lower rights, which you have the option of doing with Sandboxie. I mean, Sandboxie would have likely prevented any problem anyway. But this would have, by using the new right-dropping feature in Sandboxie. Frankly, I'm not sure if it's yet available publicly. I've been testing the beta with Ronen, and he's got it working great. So I have it. And I imagine, if it's not out, it'll be out soon. But then the DropMyRights utility that we talked about does the same thing. Basically it removes admin and a whole bunch of other privileges from the instance of running applications. And it would have shut this thing down even if you were hit by the exploit before the patch was out. I mean, and that's the kind of protection you want, real preemptive protection instead of saying, well, okay, how do I disinfect my machine after this disaster has hit?

Leo: Yeah, yeah, yeah. Another reason to use this.

Steve: Yup. It just makes sense. Samsung has had a - we have another digital picture frame malware problem. In this case it was the Samsung Model SPF-85H, which is an eight-inch digital photo frame. The frame itself is not infected. There were some before where the firmware that shipped with these was infected, such that when you connected it to your computer it could infect your machine. In this case it's the companion software disk that comes along with it which is necessary to use the frame as a USB monitor on Windows XP machines. It contains the, well, a worm. It's the W32.Sality.AE worm. And the bad news is it installs keystroke-logging malware on the machines where it has been installed.

Leo: You've got to wonder how that leaks into the production facility.

Steve: Oh, yeah.

Leo: I mean, it's on some testing machine or something, and it must be crafted to spread itself on that particular platform, I would think.

Steve: Yeah. And also to jump onto anything else you're doing. So it says, oh, look, here comes the master imprint of the CD for the digital photo frame. Let's just jump over on that.

Leo: You almost think it has to be an inside job, that somebody in the factory knew that they were going to do this production run and snuck it in there. It can't be an accident.

Steve: I mean, I agree that it's - it's hard to know what the environment is where these things are created. It may just be amateur league, wherever the software is coming from. They may be subcontracting it to some random third party. It's really not something that Samsung does. They just get the software from someone else who says, oh, you know - and they say this is what we want to do. So they take it, and they check it out, not realizing there's a trojan there. And that's a problem.

Leo: Yeah,

Steve: Microsoft reported that the most recent version of their MSRT, the Malicious Software Removal Tool, that is the December edition for last month, cleaned more than 400,000 PCs from something you have mentioned before, Leo, the Antivirus 2009.

Leo: It's amazing.

Steve: Phony security application.

Leo: Now, that's on top of some hundreds of thousands that they had removed the month before. I think we even talked about it.

Steve: Yes, exactly. So it's still spreading. And, I mean, this demonstrates that this MSRT - I've never see it do anything, unfortunately.

Leo: Well, it's almost - I have to think that Microsoft knew that this day would come. And it was like, well, let's get this thing going. Let's have it on the system. Let's keep it up to date. And now we need it.

Steve: Well, and it's so nice, too. Because, I mean, this leverages - it's proactive removal, and it leverages the Windows Update facility which, when Microsoft first introduced it, the old-timers among us were like, I don't think I want this being done all the time. Now it's like, okay, let's make sure we've got all the latest updates. Make sure we got all the latest updates.

Leo: This is done automatically. It's installed as part of Windows Update. You have it if you run Windows Update and you install critical updates. And every time they do a Windows Update it seems that they push new fixes for it.

Steve: Yeah. And so the idea is that, when you reboot your machine, this thing runs once as Windows is starting to scrub your machine of any of this. And it's not doing a big, long search that takes a long time because it's targeted. There are specific malicious things that they go directly to them and work out the details of removing them as Windows is starting. So it's free machine cleaning.

Leo: Right, right.

Steve: So that's a good thing. A little bit of bright news about how the RIAA is dealing with music piracy. They formally announced that they're changing their approach.

Leo: They're giving up?

Steve: Well, no. But they're not going to go randomly suing end-users all over the place.

Leo: Really. Wow, that's a big change.

Steve: It is a big change. A huge policy shift. I mean, they've been suing people now for the last many years. And often innocent people, some grandmother who got some trojan installed on her machine and didn't know that her machine was serving music through some peer networking system. So what they're going to now do, they've said, is work with ISPs, identify pirates, let either the ISP notify users or the ISP will provide the information, allowing the RIAA to notify users. But that will be the limit of it. They're not

saying they absolutely...

Leo: Well, but where's the stick, then? I mean, how do they enforce it?

Steve: Well, they're not saying they absolutely won't sue someone. But it will only be real gross offenders, people who, like, mass, mass offenders. But your typical end-user will get some warning notices. And they have said then that the ISP may throttle their bandwidth or take some - the ISP could say look, if you don't stop this, we're going to cut back your bandwidth, so knock it off.

Leo: So I guess the threat is that they will sue the ISP, that the ISP is in a way held liable for what its users are doing.

Steve: Well, I'll be surprised if that sticks. The ISPs want to be called a common carrier...

Leo: Right, that's not their job.

Steve: ...not responsible for - exactly.

Leo: Right. But it sounds like the only way the RIAA could make this work is if they hold, I mean, if they're not going to hold the users responsible, then it's the ISP. The ISP could just ignore them.

Steve: That's true.

Leo: The ISP could say, hey, I'm a common carrier. I'm the phone company.

Steve: And speaking of ISPs, remember that - you may remember that we covered a story about how the government of Australia was planning to do a continent-wide filtering of the Internet. Well, to say that it's met with some resistance would be an understatement. The ISPs, no ISPs want to participate. What the government has said they were going to do was to block as many as 10,000 sites that are known to be hosting illegal content. Well, Telstra, which is the largest ISP...

Leo: And partly owned by the government of Australia, I might add.

Steve: Uh-huh. And Internode, which is another biggie, both flatly said no, we will not do it.

Leo: Oh, wow.

Steve: There's another smaller one called Optus that said it would participate in some sort of scaled-back deployment, whatever that means. And then another one, iiNet, said, well, they'll participate only to demonstrate that the filtering plan will not work.

Leo: How stupid it is.

Steve: So just 100 percent backlash. I mean...

Leo: Good, good.

Steve: And there have been public protests in Melbourne, Brisbane, and Sydney that have been formal, organized protests saying we don't want our Internet filtered by our government.

Leo: Yeah. It was kind of a kooky idea. But it's not the first. I mean, remember, they spent millions designing filtering software that was cracked in a few days - in a few minutes.

Steve: Yeah.

Leo: This is crazy.

Steve: It just makes no sense.

Leo: Clearly somebody in the government has no clue.

Steve: Well, gee, you think? And Cisco released their annual security report for calendar '08 that had some interesting statistics that I thought our users would find interesting. The total number of disclosed security flaws increased in '08 by 11.5 percent.

Leo: Now, see, on the surface that sounds bad. But I think that's good.

Steve: Well, it's, I mean, it's got both good and bad to it. I mean, we're glad that these things are being found.

Leo: Exactly.

Steve: We're sorry that there are so many of them to be found.

Leo: Right. I guess my supposition is they were there anyway. They've always been there. The fact that they're finding them and disclosing them is an improvement.

Steve: Yeah. Although we're also not - I don't feel like the software we're using now is more secure than what we had.

Leo: You don't?

Steve: I mean, there's certainly more awareness of it.

Leo: I think Vista is more secure. I don't think we're hearing nearly the number of exploits on the Vista side that we used to...

Steve: Okay, but that's not a consequence of software flaws as much as it is design, where Microsoft finally really got serious about security.

Leo: True, true.

Steve: And implemented architectural features that are protecting us. But for example, all of those, that zero-day IE flaw, that affected IE, Outlook, Outlook Express, and even there were Word documents that were causing this problem. I mean, that was across all platforms except Server 2008 was the only platform that was not affected by that. So Vista was no more secure, a Vista user no more secure in this case than would a XP user be. So what was interesting was that attacks that were spread by malicious email attachments fell by 50 percent. And Cisco reported that they're seeing more and more blended attack. A blended attack, remember, meaning that there's - more than a single flaw is being used. It's sometimes multiple flaws. And in fact we'll be talking about that relative to SSL because for phishing you need both an illegitimate certificate and some way to get somebody to the wrong website. So multiple vulnerabilities being used in combination in the so-called "blend" in order to actually make the exploit happen. And finally, 90 percent of world-wide email is now spam. Nine zero.

Leo: You know, 99.9 percent of my email is spam, according to my spam service.

Steve: But Leo, you're Leo at Leoville.com.

Leo: That's great. Thanks for incurring 99.99 percent. No, no. And I've been using that address for 10 years.

Steve: Put a big beacon up.

Leo: Yeah. I mean, it's on every list there is. Interesting, though. So what they're saying is, of all the email traffic going on, nine out of 10 messages in that email traffic is garbage.

Steve: Yes.

Leo: 90 percent.

Steve: Unsolicited.

Leo: Appalling.

Steve: Unsolicited mail.

Leo: Now, remember it went down, it went down a huge bunch when they disconnected that company in San Jose.

Steve: Yes.

Leo: But I guess it's back.

Steve: Yes.

Leo: It's like roaches. You can't get rid of them.

Steve: Okay. So a couple days ago, and it was just a couple days ago, two security researchers, German security researchers Alex Sotirov and Jacob Appelbaum, introduced a surprise at a security summit. They demonstrated that they had created a fraudulent CA, a Certificate Authority, that was carrying a valid signature from a root authority.

So let's review a little bit what that means. The idea is, we've talked about the so-called "chain of trust." That is, for example, GRC's SSL certificate that I got from VeriSign, I think in this case it is signed by VeriSign. And VeriSign has their certificate signed by their root. They happen to have a - VeriSign has a root certificate authority installed in Windows. It's installed in Mac. It's installed in Linux. It's a very common certificate. So the idea is that, when someone visits GRC and wants to establish an SSL, secure, https connection to GRC, in the initial handshaking of that, after the TCP connection is established, the very next thing that happens is certificates are exchanged as part of the SSL protocol. So my server, the GRC server, sends the user its security certificate in order essentially to authenticate that they've really connected to GRC.com. So in the certificate is www.grc.com, the domain name. And so the browser makes sure that matches the URL that it was trying to get to. And then there's this chain of signatures. Basically my certificate provides the VeriSign certificate, which has been signed by the

root authority.

So the browser has this group of so-called root authority, root certificates, which are sort of like the master keys for SSL. And remember that we've talked about, in fact, jokingly but a little bit disparagingly in the past about how many root authorities there are. My system, which I keep updated with the root certificates, has 277 root authorities. And remember that I've talked about, like, for example, the Hong Kong Post Office. That's an example of one. The good news is they're secure. I will be running through a little list from my own little browsing, and also give our listeners a way that they can check their own root security certificates to see whether they are safe or not against this attack. Because many are; many are not.

So what these guys did was they set up a network of, well, first of all, to - the digital signature operates with a hash. And we've talked in years past, when we were doing our whole crypto series on Security Now!, we talked about how digital signatures work. A digital signature is a hash, a hash function, a cryptographic hash function where you take, for example, GRC's certificate, and it is hashed using MD5 or SHA-1, one of these secure hashes. And then the hash is cryptographically signed using the private key of an authority. So that creates another little blob of binary-ness. Then what happens is, to authenticate the signature of, for example, GRC's certificate, when the browser receives it, it takes the certificate, applies the hash to get essentially a fingerprint for that certificate, and it's then able - it doesn't have the private key, but it has the public key for the certificate authority. So it's able to use the public key in order to verify that the hash it gets is the same as the hash that was signed by the authority. It compares those, and that way it knows through the sequence of cryptographic operations that the certificate it got from me is the same certificate that was presented to the certificate authority and signed by them when they issued that certificate to GRC.com. And up until now there has been no way to break that process.

Well, there's been evolution in digital certificates and in hash functions over time. And an older hash function known as MD5 - MD stands for Message Digest, which is another term for a hash or a fingerprint. MD5 has begun to have some problems. Cryptographic experts over the last few years have begun to poke little holes in it, finding little things that, sort of at the esoteric far end of crypto land, were beginning to worry certificate researchers. And as a consequence, many responsible cryptographic providers began to say, okay, look, don't use MD5 anymore for things that are really mission critical. It's beginning to have problems. So far it hasn't been cracked. There have been sort of like collisions where, for example, you're able to deliberately create two different texts which, when hashed using MD5, end up with the same signature. And it's supposed to be very difficult, I mean, like really, really, really cryptographically difficult to do that. But it turns out some weaknesses cause it to be less difficult than the designers of MD5 intended.

So what happened is an additional weakness was found in MD5 using what's known as a chosen prefix attack. It's extremely computationally intensive, even with this defect. Even to exploit this defect it's computationally intensive. Now, we've talked about the notion of using gaming platforms, high-performance GPUs, the graphics processing units, in state-of-the-art graphics accelerators in order to increase the number of cryptographic operations that can be performed. What these guys did, these researchers, they took a cluster of 200 PlayStation 3 systems, so 200 PS3s, which cranked on this for two weeks. And they were able to create a fraudulent certificate authority. So what that meant was they were able to create their own certificate authority where it looked like it had been signed by one of the main root authorities. And in specifically Equifax, which is one of the oldest, been there for a long time root authorities. So they have a certificate which appears to have been issued by Equifax, but wasn't. And what that allows them to do, then, is now create any fraudulent SSL certificates that they want, apparently for any

website. It's very much like - it's like they're now a VeriSign. They can easily create certificates - www.amazon.com, www.paypal.com, anything they want. And when their certificate is presented to any browser in the world, it will be accepted. So that's not good.

Leo: Is that true for the - is it the extended certificates, too, the green ones? Or is this just a standard SSL certificate?

Steve: Well, okay, now, that's really interesting. Because what I did was to browse through my certificate store. Remember I said I've got 277 of these. And...

Leo: That's quite a cost, isn't it. That's thousands of dollars you've invested in this.

Steve: Oh, well, no. I mean, everyone has...

Leo: Oh, this is the thing that's built into your browser, not GRC certificates.

Steve: Oh, no no no. No, these are the trusted root certificates that are preinstalled in any contemporary active system. So the Mac has them, Windows has them, Linux has them. This is the way you do SSL.

Leo: Right. You have to. Right.

Steve: So, for example, and in order to browse these certificates, it's not easy. But one of the many things I have on this page, on the Security Now! Episode 177 show notes page, so again that's snipurl.com/sn177, I have instructions for how you can browse your own store of certificates. You've got to use the Microsoft Management plug-in console thing. It's a really messy UI that Microsoft came up with. But it's possible to do it.

Leo: At least you can do it. At least you can do it.

Steve: Huh? Yes.

Leo: At least you can browse it, yeah.

Steve: And so what I did was I just said, oh, okay, what's going on here? What you look for is what was the message digest, what was the fingerprint technology used for those certificates. And so, for example, the Microsoft root authority was signed with MD5. Oops. Microsoft's Authenticode root authority, MD5. Oops. Thawte's certificates are signed with MD5.

Leo: Now, they're owned by VeriSign.

Steve: Uh-huh. Although VeriSign's are all signed only with SHA-1. Equifax has both SHA-1 and MD5. And that was the one that these guys chose. So any of these roots which are signed by MD5, that have an MD5 variant, could be targets for this exploitation. There's something called Entrust.net, was MD5 and SHA-1. So but MD5 is there. That's in trouble. And, for example, the Australian Society for Data Protection has a - for some reason there's a root certificate in my machine, and it was signed by MD5. So that would be potential for exploit. On the flipside, the roots which are only SHA-1 are, for example, AOL is only SHA-1, so it is absolutely safe because as far as we know there are no known attacks against SHA-1 that there are against MD5. Comodo is also SHA-1, as are GoDaddy, GeoTrust, Wells Fargo, Visa, VeriSign, Network Solutions, and the Hong Kong Post Office.

Leo: Yay.

Steve: So they get kudos.

Leo: Yay.

Steve: The Hong Kong Post Office gets kudos for only having an SHA-1 cert. Now...

Leo: Our favorite whipping boy.

Steve: ...essentially, the guys that are still using MD5 really belong in the doghouse because MD5 has been chipping - it's been chipped away at for about the last four or five years now. And so...

Leo: So it's known that this is a flawed hash.

Steve: Well, it should have been making people uncomfortable. And it's one of those things where, you know, people who were on top of their game said, you know, there's no reason for our certificate to be signed with MD5. We're only going to sign it with SHA-1. Because even though there's nothing that we know is wrong with MD5, it doesn't seem as strong to us as we thought it was when we first signed our certs with it five years ago.

Now, one of the things that I'm noticing Microsoft is doing a lot is updating this root cert database. It is not part of the standard updates in Windows. So you need to use the custom, I think, what is it, expert mode or something they call it where you are able to look at all the things that you can update. And then it's under optional updates. And you'll see root certificate updates. And pretty much every month or two I'm seeing that Microsoft is fussing with that. So I think - I expect what will happen is that, because this is making a huge, well, I mean, yes, huge waves, as it ought to. I mean, this is not the end of the world. These guys are really good cryptographers. They built a network of 200 PS3s that it cranked for two weeks in order to create this. But as we know, the fact that

some group can do it and have now publicized this means that everyone now knows it's possible. So they seem like really good guys. They're security researchers hoping to fix this problem by demonstrating it. And unfortunately it's only by demonstrating a problem like this that many times people get off the dime and take the effort to fix it.

So what I expect to happen is that Microsoft, for example, will immediately remove MD5 from their own root certificates. And so the next update to the Windows root authority database will remove certainly Microsoft's MD5, and I imagine Thawte, GTE, Equifax, I mean, you can imagine how fast Equifax is scrambling since they're the ones that happened to get hacked because their MD5 certificate...

Leo: They're the poster boys.

Steve: Exactly. It was sitting in there and widely distributed across all the clients that are using SSL on the Internet.

Leo: Wow.

Steve: Yeah.

Leo: So does this impact other technologies using MD5? I mean, MD5 is still a widely used hash.

Steve: Well, what this says is that MD5 is clearly no longer safe. MD5 is now - it can now be said that MD5 is not just dented, it is broken. The fact that you can deploy, I mean, two weeks is not that long, even though you need 200 PS3s. I mean, you can imagine an ad hoc, some sort of, like, Internet network of PS3s, cranking along in their spare time. And there have been projects that repurposed these kinds of gaming platforms through peer-to-peer networks for searching through SETI star noise and folding of biological organisms and all kinds of different things. So you could imagine that it would be possible for other exploits using MD5. Basically, MD5 makes sense in low-security applications where you want a fingerprint. But having said that, and given that SHA-1 is so available...

Leo: And so effective and uncracked, yeah.

Steve: Exactly. Why not use it? I mean, I think this is the death knell for MD5.

Leo: It's a big shock. So is there anything people can do at this point? I mean, there's no, I mean, all these certificate authorities have to change their technology; right?

Steve: Yeah. I would say, I mean, if somebody were - if you were the CIA or somebody who was really concerned, what you could do is go through your root store - and again, on the show notes for Episode 177, snipurl.com/sn177, I will show our users how to do

this. I'll see if I can do it on the Mac. I'm not nearly as familiar with the Mac as I am with Windows. But it's certainly possible to look through the root certificate store. And users could delete any of the certificates that are signed using MD5. And in doing so, they have essentially said to their computer, okay, this computer is no longer going to accept MD5-signed certificates. Which, you know, it does solve the problem. You may find that if there were a website that didn't have, for example, both MD5 and SHA-1, if it was only signed with an MD5 cert and not co-signed with an SHA-1, then you may not be able to connect with SSL. And then you'd have to decide if you wanted to or not. Now remember, this, however, would only be used as part of a blended attack. So two things are necessary. You would need not only to be able to have a spoofed certificate offered by a server, that is, the destination server that you go to, but also some way of diverting you to that. Now, as it happens, earlier this year we talked about DNS spoofing and the so-called Kaminsky Attack, which does exactly that.

Leo: Aha.

Steve: So, yes. So we were saying that, okay, so you go to a site which is a spoofed site, thanks to DNS being poisoned. And okay, well, fine, maybe you don't notice that when you're logging into eBay it hasn't switched you into a secure mode. And if they don't switch you to SSL, and you just assume that the login is going to take care of your security because it always does, then you're using a spoofed server, and SSL doesn't come into play at all. But if you were very security conscious, you might make sure that you were at https://www.ebay.com, or PayPal or whatever, and you could even then, as we've often said, check to make sure your lock is unbroken or your key is unbroken. Right-click on the page, make sure that you're secure. All of that would work if the server had a fraudulent certificate issued by a fraudulent certificate authority. So two things are necessary. It's not just the spoofing of the certificate. It's also somehow getting you to a fraudulent server with a fraudulent certificate. So both things are necessary. Although both things are potentially possible.

Leo: Hanging out there.

Steve: And 25 percent of DNS servers have still not been fixed.

Leo: Is that the number still?

Steve: Yeah.

Leo: Geez, Louise.

Steve: One out of four.

Leo: Use OpenDNS.

Steve: Exactly.

Leo: Let's talk about the PDP-8. I remember, when I first started working at a radio station in 1987 in San Francisco, KNBR, they were doing their music programming with a PDP-8. And I thought, this is so antiquated. This is '87.

Steve: Well, the very first computer I ever saw, I must have been, like, 10. And my dad took me to his corporate computer facility. He worked for Industrial Indemnity in San Francisco, big industrial insurance company. And this was the guys walking around in the white lab coats on the raised floor. The whole facility was like it was a little jewel. It was, I mean, it was a showpiece for the company. And so we went down, and of course there was no going in the room. I just sort of pressed my face up against the window, which was cold because it was all air conditioned on the other side. And I was just mesmerized. Here was, I think it might have been an early IBM 360 because it had a huge panel of lights, the buttons all over the place. I mean, the classic sci-fi-looking, what people think of as like an old-style computer with all literally active twitching reel-to-reel tape drives, a pair of reels, and then the vacuum loops that were used for mechanical buffering because the tape would be twitching back and forth, and then these vacuum loops would be used to drive the reels back and forth. And, I mean, just - and a big huge line printer going ching-ching-ching-ching-ching-ching-ching, moving through paper very fast. I mean, I was just - it was like love at first sight.

Leo: Now, that was a mainframe; right?

Steve: That was, oh, yeah, that was a full-on, major league mainframe. And back in a time when machines like that were still very expensive and very new. But a big industrial insurance company like Industrial Indemnity, they live and breathe with managing all of their accounts and accounting and had the kind of money to afford that. So that's...

Leo: This was a huge breakthrough, really.

Steve: Yeah. So that really sort of set me off on, well, I mean, I was already - I knew computers was where I was going to be. At that point I was very involved in electronics. You know, my dad took a picture of me before I was five years old wiring up stuff in the backyard. We had a picnic table, and I was wiring buzzers and bells and knife switches and things.

Leo: Why am I not surprised?

Steve: I was a computer hobbyist from the beginning.

Leo: If you could have made your doorbell go "yabba-dabba-do," you would have.

Steve: And then when I was in high school I used to hang out in the math resource center, I mean, serious geek, nerd person.

Leo: Nerd, nerd.

Steve: And one of the high school teachers told me about a company in San Carlos that was located not far from San Mateo, where I was, that was doing something with computers, and that maybe there was an opportunity there. And I thought, well, I've got to go find out about that. So this was a company called Technica Education Corporation. And it was there that I actually encountered and touched my very first computer, which was this Digital Equipment Corporation, DEC, PDP-8e. And it was a 19-inch-wide, rack-mounted thing with switches on the front and lights. And this was my first computer.

Leo: You can't underestimate the importance, by the way, I think, of that human scale. Going from that thing that was isolated on the other side of the glass, and the high priesthood was maintaining it...

Steve: Exactly.

Leo: You had no accessibility. When you're suddenly touching a computer, the whole thing changes.

Steve: Oh, yeah. It was, I mean, I want to say a religious experience.

Leo: Yeah.

Steve: I mean, it was just like, oh, my god. I mean, here it was...

Leo: Well, you're not alone. I think Bill Gates, the PDP that he used at Lake School, Lakeside School, that's what turned him on.

Steve: Yes. Well, and there was the ASR-33, the classic teletype that had the big, round, sort of cylindrical keys you would press down one at a time.

Leo: [Sound effects]

Steve: Yeah, exactly. And it went 10 characters per second was as fast as it could go. Then over mounted to the left of it was the paper tape punch and reader. So because, you know, you loaded software on eight-channel, eight-track paper tape. There was a guy there who was - so I was probably either a sophomore or a junior in high school, so 15 or 16. There was a guy there who was a few years older than I, guy by the name of Lynn Cooley, who at the time had, like hippie sort of long, blonde hair tied in a big pony tail. And he had a job at Technica, where I was soon employed. And it was Lynn who sat down with me and said okay, let me show you how this works.

Leo: Oh, that's neat.

Steve: And I learned Assembly language, the very first Assembly language, on the PDP-8.

Leo: And you never stopped.

Steve: Oh, and I never stopped. I'm still programming Assembly language. That's my language of choice.

Leo: What was the Assembly for PDP-8 like compared to the 8086 Assembler that you - the x86...

Steve: Oh, well, it's funny. Minicomputer, we think of mini as meaning "miniature." But they called it a minicomputer. They meant it as "minimal." That is, it was deliberately a minimal computer. That is, the least computer that you could have and still be a computer. So, for example, there's no load instruction to load from memory into the accumulator. Instead you can add what's in the accumulator - you can add a memory location into the accumulator. Which means to do a load, you have to do a clear the accumulator...

Leo: Zero it first, and then you add.

Steve: Zero it and then add. There's no XOR. There's no OR, believe it or not.

Leo: Wow. What?

Steve: Those fundamental logical operations.

Leo: But you can simulate all of them with multiple steps; right?

Steve: Exactly. And so the PDP-8 is a 12-bit machine. That is, you know, we're used to 16 and 32 and 64. This thing is 12 bits. And there was a lineage of 12-bit machines that DEC produced over time. The first three bits of the 12-bit word is the opcode, meaning there's eight of them.

Leo: That's eight things it can do.

Steve: Yes. Now, eight fundamental things. So, for example, there's add...

Leo: Add, subtract, there's got to be a move; right?

Steve: No.

Leo: A compare? There's a compare.

Steve: Well, one of the opcodes has - is like a lot of little bits down below. So, for example, there are things like complement the carry, complement the accumulator, those sorts of things are all variations in one of the opcodes. And one of them is an I/O instruction. So you have I/O. You have that math. There's the...

Leo: Right. No multiply, probably, just add and subtract.

Steve: Oh, yeah. No multiply. Oh, my god, you were just dreaming if you wanted to multiply. There's an instruction called DCA, Deposit and Clear Accumulator. And you don't have a choice. So anytime you store data in memory, your accumulator is cleared.

Leo: Oh, man.

Steve: So if you want to store it and not have it cleared, then you've got to store it and then do the TAD, which is that add instruction. But the accumulator is cleared now, so when you add back what you just stored you get it back again. So the point is it was really, really minimal. There's no stack in this machine. They hadn't invented stacks at the time.

Leo: Wow.

Steve: But what it was, was a perfect platform for playing around with a computer. I mean, this was...

Leo: Well, it was a personal - it was the first personal computer.

Steve: Yes. Well, yes. I mean, it was personal. I was able - I don't think I slept for about three weeks after I had access to this machine. I didn't want to sleep. I didn't want to eat. I didn't want to do anything except - and it had a front panel and lights, just like the big one that I had seen behind the glass. And so you literally, when you - it also had core memory, so actual ferromagnetic little doughnuts in there that were magnetized one way or the other. And everything worked with core memory. There was no - we didn't have solid-state memory back then.

Leo: And how many words did you have? Probably not a lot.

Steve: Well, okay. !2 bits can only access 4K. 4K.

Leo: Yeah, but 4K probably costs thousands of dollars when it's core.

Steve: Oh, yeah, yeah, yeah. This thing was - it was, I think, like a $25,000 minimal computer at the time.

Leo: Unbelievable.

Steve: It was expandable. They had, like, a bank-switching arrangement. You could expand it, so you could have eight 4K banks, meaning the absolute maximum configuration was 32K. 32 kilobytes, or kilowords. So anyway, I was just, I mean, that was my first machine. And obviously it had a warm spot for me. I mean, it's meant a lot over time. So you are actually responsible, Leo, for what happened next. I was watching TWiT Live, and somebody on camera brought out a core memory plane.

Leo: Me. I have one.

Steve: You've got one, I know, somewhere around there.

Leo: Yeah.

Steve: And I don't know what I was doing. I was working or doodling or something. I just had TWiT Live on in the background. And there was this core memory plane. I looked at it. I thought, I want one of those.

Leo: Had you told me, that could have been your Christmas gift.

Steve: I don't have any - well, I've got core now. But so I thought, I need some core memory. Just, you know, because. Before it all goes away. Before it's all been...

Leo: Yeah. Somebody sent - they framed it, and they sent it to me.

Steve: That's so neat. So of course I went to eBay, and I put in "core memory." And there was a bunch of people selling core memory. So I got a couple different ones. And there was one that I struck up a dialogue with this gal in West Virginia, a surplus seller. And I don't remember now what it was, maybe we were talking about shipping, or maybe I bought two of them, and I thought, well, I'm going to get these two, why don't you just put them together and ship it to me in one box and we'll save some money or something.

So we're sending email back and forth, and she says, by the way, I also have a couple PDP-8s with core memory. And I said, what? You have what? Okay, now this, you know,

this was 35 years ago that this was all happening, or more than that even, maybe 40 years ago. And I said, what do you mean, PDP-8s? They're all gone. She says no, I've got a couple in a couple crates. So I thought, okay. Send me pictures. So she didn't - she wasn't sure what they were. They were two machines, each in their own crate. And she took a picture of the front panel. And sure enough, it's a PDP-8. But it wasn't a completely standard PDP-8. There was something different about the panel. Well, Google is your friend. I was able to figure out that these PDP-8s were part of a Canadian LORAN-C monitoring network.

Leo: Whoa. This is...

Steve: LORAN-C is a land-based navigation system, sort of old school. And what's interesting is that until the attacks of September 11, LORAN-C was going to be decommissioned because now we have GPS.

Leo: Right.

Steve: But the Department of Homeland Security decided that we might need a backup positioning system. So they decided not to scrap LORAN-C because the advantage of LORAN-C is it's completely different from GPS. GPS is satellite based, uses a completely different frequency range. LORAN-C is much lower frequency. GPS is very high frequency. LORAN-C is ground-based as opposed to space-based. So it made sense that this would be a good fallback navigation system. So I learned from doing some Googling that these machines had been integral to - had been designed into these monitoring stations years ago and had been decommissioned.

And in fact there was a letter I found where someone said that they, when they tried to remove the PDP-8s, because these were such old machines, and just like replace them with something new, they found that they - it was a much, much harder job than they anticipated because the PDP-8 wasn't monitoring the receiver. It was the receiver. That is, it had been integrated so tightly into the electronics that it was involved in all aspects of running the receiver. What these were, these were fixed-location stations that received the LORAN-C transmissions and just checked them. They were just verifying that what the various LORAN-C transmitters were sending was correct. So they were doing the sort of like land-based quality control. Well, what I then found out was, to my amazement, these two machines that this gal in West Virginia had had never been used. They were...

Leo: Really.

Steve: They were spares. Brand new, never deployed. They've been sitting in Alameda County at the U.S. Coast Guard in Alameda for who knows how many years.

Leo: And presumably maintained and kept dry and, I mean...

Steve: Well, yeah, I mean, in individual crates. They were crated, ready to be sent out to replace a broken deployed PDP-8e in one of these monitoring stations, if that ever

happened. So I own them now, needless to say.

Leo: You bought the whole thing.

Steve: How could I not? I mean, this is a piece of history that - and it's funny, too, Leo. Because, I mean, whenever I look at the photo of the front of one of these, I just kind of like, oh, god. I mean, it just...

Leo: Isn't that neat.

Steve: It really gets me. Okay. So the reason this is interesting for, or potentially interesting for our listeners, is that something else happened while I was doing all this PDP-8 research. I stumbled on a site, SpareTimeGizmos.com, by a neat engineer who's also a programmer PDP guy. DEC did a bunch of different PDPs. There was the PDP-10 actually I encountered when I was working at the AI lab at Stanford. They had a PDP-10, and I think they used a PDP-11 as the front end. So PDP stands for Program Data Processor. Anyway, this guy Bob Armstrong created a PDP-8 kit toward the end of the life of the PDP-8 line. Intersil, that was a semiconductor manufacturer, created a PDP-8 on-a-chip, a single-chip PDP-8.

Leo: Probably not such a sophisticated chip either, given what you've told me.

Steve: Probably not that difficult to do; right. And Harris Semiconductor later bought Intersil. They produced the HD-6100 was the name of their chip, and then a second-generation HD-6120. Well, Bob Armstrong, who is sort of a hobbyist/craftsman/kit builder guy, he's got a whole bunch of cool things on his site. One of them is a - he calls it the SBC6120, Single Board Computer 6120, which is - it's about, I don't know, four by five inches. And it is a complete PDP-8 kit with a serial interface and, nicely, an IDE interface. So you could interface this PDP-8, which is a - it runs all the standard DEC software. DEC has done something interesting, too. All of the software has been preserved. All the manuals have been preserved. BitSavers.org has all of this. And there are various PDP-8 hobbyist/enthusiast sites around the 'Net where there's been an active effort to preserve this and keep this from being lost.

Leo: Now, would you power yours up, your LORAN systems up? Or are they just going to sit under glass in a museum?

Steve: Well, it's interesting. We're going to be talking about capacitors of a different sort here next. What happens with unused electrolytic capacitors is that...

Leo: They leak.

Steve: They die. And the old-style power supplies, so-called "linear power supplies," or you could almost think of them as, like, analog as opposed to digital power supplies. Contemporary power supplies are almost universally switching power supplies. The

original old linear power supplies have typically very large silver cans which are electrolytic capacitors, which are essentially the technology we have for creating a lot of capacitance in a reasonable space at a low voltage. They rely on aluminum oxide as their insulator. And over time the aluminum oxide breaks down in the capacitor. So it's very likely that, were I to simply plug these machines in, they would explode. The capacitors would explode.

Leo: Oh, dear.

Steve: Fuses would blow. Rectifiers would blow. I mean, not something you want to have happen to your Model T prize antique of your life. So it's possible, though, through a process of restoration - it's called "reforming" a capacitor. You take the capacitors out one by one. You give them a little bit of voltage and run some current through them. And they will replate themselves. They will...

Leo: Oh, so it's not a leak. It's just they got deplated.

Steve: Yes. They've been deplated. Unfortunately, if you put them under full use load, they would be short circuits. And what happens is that a current would flow through, then it would burn the capacitor in that spot, and it would never be fixable again.

Leo: So you're just going to trickle something into it so that the surface replates itself, essentially.

Steve: Exactly. So you run a controlled current of a couple of milliamps through the capacitor. And over time you'll see that - in fact, what I'll use is I'll use a constant current lab bench supply. I've got one, and so I'll set it to - I'll limit its current to a couple mils and then set its voltage to the rate of voltage of the capacitor. So over time it'll slowly bring the voltage up on the capacitor as the current running through it is kept constant. But as it's replating itself it'll eventually become an open circuit again. It'll end up essentially no longer leaking. And that capacitor will have been fixed. And so I'll step through every single large filter capacitor in the power supply, one by one, bringing them back to life, essentially.

So anyway, so I do certainly - I'm interested in making those machines work. But I'm also excited, or I was excited, about this notion of there being a kit. The problem was that when I went to this site, this SpareTimeGizmos.com, this was years ago it had been done. The kits used to exist. I think they were discontinued maybe in '04. So Bob had created this, I mean, literally a turnkey kit - circuit board, all the components, everything you need, buy it from him, sit down on a Saturday afternoon with a soldering iron and build yourself a working PDP-8. Then he went the next step. And he created a front panel for this thing.

Leo: I see it on the site. It's so funny. It doesn't say PDP-8.

Steve: I think he calls it, what, Gizmos?

Leo: It says Gizmo SBC6120.

Steve: SBC6120. Yup. So that is a working control panel that emulates the PDP-8, just like what I had when I was 15, and what I may have...

Leo: Now, do you flip those switches to program it?

Steve: Yes. Yes. I mean, for example, when the machine is empty, and you want to read in a paper tape, you have to key in the so-called "boot loader." So you flip the switches...

Leo: How many switch flips is that?

Steve: Oh, it's not that many instructions. I think it's maybe like 12 or 13 instructions. It's a very simple loader that is simply - it simply says read the next chunk of - read the next data from the paper tape. Store it here. Read the next one. Store it there.

Leo: But you're flipping those switches essentially with binary code for the Assembly instructions.

Steve: Yes. Yes. And in fact that was what...

Leo: It's a great way to learn about computers, frankly.

Steve: Oh, well, in fact, Leo, many universities teach, I mean to this day, teach Assembly language using PDP-8 emulators.

Leo: Interesting.

Steve: I mean, the PDP-8 has been emulated. There is courseware about the PDP-8. If you put into Google "PDP-8 programming," you'll find page after page about the PDP-8 and programming because it's a perfect machine to learn programming on. And this front panel, it's got the lights and switches just like the original PDP-8 did, where you're able to, like, flip the switches and then press Load. And so it stores that and steps to the next instruction. Flip the switches, press Load, literally to key in a little program. And then it's got a switch that says Run. And you press Run, and the machine runs it. I mean, it's a real, honest-to-god little computer.

Leo: Very neat.

Steve: So anyway, what happened was I was mourning the fact that four years ago this had happened and I didn't know about it, because I would have loved to have had one of

these single-board computers, and certainly this fantastic front panel to go along with it.

Leo: That's the real reason. Because, frankly, you could do it all in software. I mean, you could run a PDP-8 on any modern computer system easily.

Steve: An emulation of it, certainly.

Leo: Yeah, yeah. But you want the flip. You want the switches.

Steve: Oh, yeah. Well, and it's so thin now that you can literally get sort of like a deep picture frame, and you could hang it on the wall.

Leo: You're right. It's not - I'm looking at. You're right. It's not a big old box, is it.

Steve: No, it's only - I think it's maybe, what, maybe four or five inches deep.

Leo: Because it's just that little board is all that's in there.

Steve: It's just a little board inside. But, I mean, but Bob did - I mean, he's a craftsman. Those front panels, they are multicolor silk screen. They are laser cut panels. I mean, just beautiful work...

Leo: I've got to get one of those. That is awesome.

Steve: Well, in fact, Leo, what I'm going to tell you is, I don't know if your builder gal...

Leo: Colleen?

Steve: Colleen, yeah. I don't know if Colleen wants to build it. But if you want one, and she doesn't want to build it, I will build it for you.

Leo: I'll probably - but I can - I'm not an idiot.

Steve: Okay. Well...

Leo: Is a little soldering involved? There's a little soldering?

Steve: Lots of soldering, yes.

Leo: Lots of solder. Oh, because you have to put all the chips and everything on the board.

Steve: Yeah.

Leo: Oh, okay.

Steve: Anyway, so what happened was, I was shedding a tear, I mean, yes, I was going to get some real PDP-8e's. But this was just like portable, low power, it would really work, brand new. And it was just a work of art that this guy had created. So anyway, I wrote to Bob, and I said, hey, Bob, I've seen your site. I realize this was years ago; it's too late. I said, if you know anyone who wants to sell theirs, I'm definitely in the market. I'd be happy to buy one. I think in fact maybe at some point he put them on eBay. I'm not sure, but I saw some reference to eBay. Also, all of his work is open source. That is, he's not trying to make any money on this. So, like, all the software, all of the Gerber tapes for making the circuit boards, I mean, he's just said, if anyone wants to do this much more on their own, they're welcome to. But otherwise he was producing a kit. So I wrote to him and I said, for what it's worth, I don't know, if ever one - if one comes along, if someone wants to sell theirs, if it ever comes back to life, absolutely put me on some list. I have to have one. And so I got email back from him a couple days ago, I mean, a couple days after that that said, well...

Leo: Colleen has just come in to say I want to build one. I don't know why. She never would have seen anything like this. For her this is like the Dark Ages.

Steve: Oh, but it's just such a slice of history.

Leo: She wants to do it.

Steve: Good. So he said we may have some news by the end of the year, if not sooner. And sure enough, somehow - see, this chip that's the heart of this is this Harris, this HD-6120. And they haven't been making them for 15 years. I mean, it's been dis- it's long since discontinued. Somehow Bob got some more. And there's been enough pressure on him to, like, bring this thing back to life that for a limited time it's going to come back to life. And I've told him I need three.

Leo: [Laughing]

Steve: I don't know why. I mean, two, you know, because it's going to go away, and it's never...

Leo: I want to do a Beowulf cluster with my PDP-8.

Steve: It's never - it's going to go away, and it's never going to come back again.

Leo: No, that's true.

Steve: I mean, this is never going to happen again because when these chips are gone, they're completely gone.

Leo: I would just buy the front panel and hang it on the wall here and pretend.

Steve: Well, Leo, you've got to have the lights blinking.

Leo: Oh, yeah, you're right.

Steve: And so what I'll do is I'll write a little program for you that makes blinky lights.

Leo: So it's 350 bucks for the full kit. So that's the board; that's all the parts. You have to solder them, though, onto the board.

Steve: Oh, yeah. It's not for someone who's not comfortable building things, building electronics. But that does not include the front panel. The front panel, he needs to see whether there's enough interest. At this point he's got a Yahoo! Group. I've got links on our page. But he also, down in the lower left-hand corner of his page, he talks about Yahoo! Groups. There's a SpareTimeGizmos Yahoo! Group. I've joined the mailing list side. You can just send sparetimegizmos-subscribe@yahoogroups.com, I think is the address.

Leo: No, I've got to have one. I've got to have one of these. I've got to have one of these.

Steve: It looks like about 15 people so far have said, oh, absolutely, I need a front panel. I need three front panels because I want one for each of my little boards.

Leo: I would like to automate my home using this device.

Steve: Well, it is expandable. It's got a bus on it, so you can do that. It's also got the IDE interface. And remember that IDE is the same as Compact Flash.

Leo: Right.

Steve: So you could just take a little 1GB, inexpensive Compact Flash and have

nonvolatile storage. Also the other guys that have paved this road already, they've got the various - all the DEC software is in this format. OS/8, which was the operating system for it, is there and running on this.

Leo: Would I need a paper tape loader? Or how would I get - I guess I could put it on the Compact Flash.

Steve: Yeah. I haven't followed through all the details.

Leo: That's going to be interesting, yeah.

Steve: It has a serial interface also. So you could also connect it to your PC or your Mac and then use a terminal emulator in order to talk to it. But one way or another we'll do this. So it runs OS/8. FOCAL 69 was the formula calculator, was the language that the DEC created back then for these machines. And a whole bunch of stuff. And, I mean, for anyone who is interested in, like, a chunk of history...

Leo: No kidding.

Steve: ...who, you know, the idea of switches and lights on a real little computer, something very understandable. The original books, the handbooks are still available online. Everything has been scanned and has formally been released from copyright by DEC. So you can get PDP, I mean, you can get PDF files of all the documentation. It's just - and anyway, I just wanted to tell our listeners. I don't know how many old-timers we've got.

Leo: That's so cool. Did he say how many people he'd need to get to order that front panel?

Steve: He said 100. 100 would...

Leo: 100. And how much would it be?

Steve: I think it's going to be, like, $400, or $450.

Leo: For just the panel.

Steve: For just the panel. So I'm not sure, but...

Leo: So you're talking 350 for the guts and 400...

Steve: Yeah.

Leo: 750 bucks to build a computer that is essentially dumber than my digital camera. Or, I mean...

Steve: I know. It's nuts. But it - I want...

Leo: I understand. I understand.

Steve: I felt such a sense of loss when I thought I had missed the window, that this had happened, and it was never going to happen again. Now it is. So I wanted to take some time to tell our listeners. Based on the reactions just in my own newsgroup, because I've told the GRC newsgroup about this, there were a bunch of people, like, oh my god, that was the first computer I encountered. Or we had one at work. Or just like you said, you had one at the radio station.

Leo: Sure.

Steve: That was still doing something.

Leo: Well, we've got 75,000 people listening. I bet we could find 100 people listening who would want to build one of these.

Steve: We'll find out. Because again, all the links are there. You can go to SpareTimeGizmos.com or Security Now!'s Episode 177 page that I've mentioned, snipurl.com/sn177. I put a bunch of notes up there. Contact Bob. Join the SpareTimeGizmos Yahoo! Group. Send email saying, hey, I'm onboard, I want to do this. And we'll see how many people we get.

Leo: What a hoot.

Steve: It just is. It's a kick. And Leo, I could just see it in the background there on the shelf.

Leo: Well, that's what I'm thinking, exactly. Having it blink there, right there, it's a piece of history.

Steve: Such a piece of history, yes.

Leo: Well, maybe we'll - Colleen really wants to build it. The problem is it's one of those things that, oh, I would love to do that. But it's just, you know, it's hours and

hours and hours. Not merely the building, but understanding it and hooking it up. And it's a big commitment.

Steve: I can't think of anything more fun. Actually, I have to tell you. When this happened, when it turned out I could actually have a couple of the real antique PDP-8s, and not even knowing that I'm going to be able to get one, I mean, definitely the boards are available. So there's a real piece of PDP-8 hardware. My plan...

Leo: Well, you've got a PDP-8. You've got a couple of them already.

Steve: Yes. My plan, when the world has decided it no longer needs me, when it turns me out to pasture, you know, in 30 years...

Leo: You'll be the dotty old guy in the nursing home...

Steve: When I'm 83, yes.

Leo: [Indiscernible] make it work.

Steve: My plan is to start from scratch and write everything for the PDP-8.

Leo: SpinRite?

Steve: An editor - no. I've never taken an empty machine and created an entire environment - editor, assembler, compiler, operating system, everything.

Leo: That's what Kernighan did with UNIX. I mean, that's - you sit there. Here's the hardware. We need, you know, everything.

Steve: Right, right.

Leo: I mean, there is exists - you could use OS, as you said, OS/8. But I think fun, I mean, really fun project.

Steve: And, I mean, it's not interesting to do it on an Intel chip. First of all, there isn't documentation for, like, everything. I can't write from scratch a driver for my graphics card because they just give you the drivers. And that doesn't - it doesn't interest me. It's too easy to do that for a contemporary chip. But imagine, like, a real editor, a full-screen editor, an assembler, an operating system for a chip with no XOR and no OR, where you have to do a combination of instructions to do that. I mean, no stack. It'd be a real, I mean, I'd be sitting there with a pencil thinking, okay, how am I going to do this now on

this thing? Anyway, I just think it would be a really, really fun puzzle for, like - I'll have come full circle. The first machine I ever saw and the last machine I ever program, both a PDP-8.

Leo: I remember this. Oh, I love it. So it's all there. We have snipurl.com/sn177. You can go there to get all the details.

Steve: And you see pictures of it immediately. I put a picture of this beautiful thing on our site, and you can also see it on Bob's site at SpareTimeGizmos.com.

Leo: Before we get to the capacitor story, I just want to mention a story that's breaking now as we record. We're recording this the last day of 2008. You're going to hear this the first day of 2009. Apparently Zunes stopped working at midnight last night. They're calling it Z2K.

Steve: Oh, no.

Leo: Microsoft says, yeah, we know there's a problem. It's apparently only affecting the 30GB Zunes. I have a 4GB Zune that's not. But many of them just frozen up. Some people are reporting that popping the battery and restoring the system essentially to earlier firmware - it's apparently a firmware issue. Can you imagine the nightmare that Microsoft - first they've got this Red Ring of Death on Xboxes. And now this. The Zune just stops working on December 30, 2008. Unbelievable. Let's talk about capacitors.

Steve: Yes. Okay. I've sort of been watching energy stuff, sort of in the background, for quite a while. I'm one of these people, I've read a bunch of books about various topics surrounding this issue of peak oil. You know, are we going to get to a point where oil availability is going to become a problem. And I'm not an apocalypse guy. I don't think the end of the world is going to happen. Obviously we're not going to suddenly run dry of oil. But the earth originally had about two trillion barrels of oil. And we've pulled about one trillion out of it, about half. And the...

Leo: Right. It gets harder and harder, of course, to get.

Steve: Yes. And, well, we've got the easiest...

Leo: We got the easy stuff, yeah.

Steve: ...one trillion. You know, this all began when some farmer in Pennsylvania was pissed off because there was black goo coming up in the middle - it was, like, upsetting his crops. And of course the rest is history. So until 1970 the U.S. was a net exporter of petroleum. I mean the whole Texas Tea, I mean, we've got grasshoppers pumping on stuff over here in Southern California even. But what happened was the U.S. hit its peak and has been in production declining ever since. We still produce oil, but we don't have

enough to export to the rest of the world. And of course Saudi Arabia is the famous producer now. Their fields are aging.

Anyway, the point is that long-term, at some point we're going to have a problem where we're no longer able to grow production, even though consumption is still growing. And it is still growing. Now the worldwide economic slowdown that we're one year into in the U.S., I mean, that's certainly going to slow down demand. It has slowed down demand. And in fact last summer's high prices slowed down driving a lot, and so demand got cut. So it's impossible to know when this is going to happen. And when it does, it's not like the oil's gone. It's just like, wait a minute, now we'd like to have more than we're able to get. And so you can imagine prices are going to go up and probably stay up. They're not going to be - there's no way they're going to go back down again to the level that they have again.

So this puts a lot of pressure on alternatives. Certainly we can get a lot more efficient. Cars can get much more fuel-efficient. We've seen the hybrid model where it's a hybrid electric and gas. There's wind and solar and so forth. But one of the problems with cars is batteries because what many current hybrids have has a limited life. It lasts maybe three years, and then it needs to be replaced.

Leo: It's also - they're also very heavy. The Tesla has a thousand pounds of battery in it.

Steve: And they cost about half the price of the car, Leo.

Leo: Right, right. And they're explosive. And they take forever to charge.

Steve: They take forever to charge, and they're toxic. I mean, lithium is not something that you want out in the environment. Lithium-ion cells, I mean, and lead acid is the same way. All these battery technologies have serious downsides. But one of the things that I noticed was people are talking about if Detroit ever survives and gets its act together and is actually producing electric vehicles, as I understand it they're talking about you buy the car, and you lease the battery. That's how they're going to solve the problem of these things having limited life. But the lease charge is, like, $200 a month is the lease on the battery. But that way you don't own the battery, so you're not upset with the manufacturer when it really no longer gets you over to the market any longer.

Leo: Plus they can force it to be recycled and so forth.

Steve: So against this background there's been operating in Cedar Park, Texas, some sort of a company under wraps of secrecy called EEStor, Inc. EEStor, all that was known about them was that they had some amazing next-generation energy storage technology.

Leo: Now, this isn't like those guys who claimed I can run my car on a teaspoon of water, is it?

Steve: Well, no. The reason I'm excited, the reason I'm taking our listeners' time with this, is you know I'm a double-E. As I said, I was wiring electrical things before I was five years old. And it was all hardware until I switched over - in fact, when I was at Berkeley, people used to say, oh, are you hardware or software? It's like, you know, you couldn't be a hybrid. You were either a programmer or you were a nuts-and-bolts guy. But those people didn't know about computers and software, and the software guys didn't know about the hardware. I had the advantage of sort of having come through both eras and was able to mix it. Which actually is probably where SpinRite came from. But what excites me about this is that it makes sense. I once heard the notion of a supercap, a supercapacitor. And I thought, wow, that's a neat idea, the idea of making a bigger capacitor, a capacitor that would store more energy.

Leo: So, but you have to understand what a capacitor does for this to be...

Steve: And we're going to talk about that.

Leo: Okay, okay.

Steve: So this company, no one really knew what they did. There were some press releases. People I think knew that they were funded by Kleiner Perkins Caulfield & Byers. Well, Kleiner Perkins, as they're known, is one of the more successful venture capital firms in Silicon Valley. They have, for example, financed little companies called Google and Amazon and Netscape and AOL. I mean, these guys tend to know what they're doing. They do make some wild bets, but with potentially wild upside.

So what happened, what finally brought this to my attention is on Tuesday, December 16th of this year, a few weeks ago, U.S. Patent 7466536 was granted. And as happened with a granted patent, the content of the patent is then put into the public domain. The inventors or their assignees have 17 years of exclusive rights to the intellectual property described in the patent. But part of the idea is - the idea is that other people can build on that. So it's made public. The title of the patent is "Utilization of Polyethylene Terephthalate Plastic and Composition-Modified Barium Titanate Powders in a Matrix That Allows Polarization and the Use of Integrated Circuit Technologies for the Production of Lightweight, Ultrahigh Electrical Energy Storage Units." Which is a mouthful.

What these guys have succeeded in doing is using integrated circuit production technologies and essentially nanotechnology to revolutionize capacitors, the fabrication of capacitors. Okay. Now, a capacitor in its simplest form is - you can visualize it as two parallel plates that are spaced close together, that are connected, and there's a wire running from each plate off to somewhere else. The characteristic is there is no flow of current across the plates because they're separated, like by an insulator. The insulator is called a dielectric in the case of a capacitor. But an electrostatic field is created when a charge is placed on this. That is to say, if you were to hook this up, this capacitor up to a battery, like maybe through a light bulb or some resistance, the voltage in the battery would flow through the circuit, essentially charging the capacitor. So the battery would give up some of its energy to this capacitor, which stores the energy in the form of an electrostatic field between these plates. So the amount of capacitance is a function of the size of the plates - the bigger the plates, the more capacity in the capacitor - and the proximity of the plates to each other. The closer together they are, the greater the capacity.

Now, the amount of capacitance in a capacitor is measured in something called a "farad." And the problem is a farad is impractically large. So all the capacitors I have in the garage, the capacitors we've got in our computers, they're microfarads. You might have 25 microfarads or 100 microfarads. Or maybe 250 microfarads. That is to say, millionths of a farad, because the actual value of a farad represents so much capacity that no one's created capacitors in high volume and practical applications that are many farad before. So, and these typical capacitors we have in our consumer electronics will maybe have, like, a 25-volt rating, meaning that the way they're built, they have, for example, 100 microfarads of capacity at 25 volts. So you can put 25 volts of charge on the capacitor, and that's all the manufacturer is guaranteeing them for.

If you crank them up much above that, what voltage is, and to use a water analogy, voltage is pressure. So current is the actual flow of electrons. Voltage is the pressure behind that flow, if any. You may not have any flow. You might just have pressure. For example, if you were, like, holding a garden hose closed, you could feel the pressure even though there's no flow. Current is the actual flow of the water from the hose. So you might be able to have 25 volts on this 25-volt capacitor. I'm sure there's some leeway, some headroom. But if you went way higher, this thing would end up overheating because you would - essentially the voltage would end up creating a stress in the capacitor that would cause a perforation through this dielectric which is insulating the two sides of the capacitor.

And if people are familiar with the way these things look, they typically look like little tanks. What they actually are typically is two pieces of long aluminum strip, which is then rolled up. And it's really - it's interesting. It's rolled up because then you get sort of the effect of interlacing plates. If you don't have just two plates, but if you roll those over on themselves, then you have the electrostatic field sort of on both sides of alternating plates in order to form the capacitor.

Okay. So what these guys have done is they've been working in quiet in Cedar Park, Texas, for many years. They're about a year behind schedule. But little bits and pieces have been coming out. For example, Lockheed-Martin, the largest aerospace contractor in the United States, has an exclusive contract with them now for military and aerospace applications. So that sort of lends a little bit of credence to what these guys are doing. Also they're clearly working in the right area because Georgia Tech has been working with the same, this barium titanium oxide, which is known as barium titanate, is the material used as the dielectric. It's a nanoparticle-fine powder that has extremely high breakdown voltage. And that's what you want. You want to be able to put as much voltage in a capacitor as possible. And the measure of energy that you can store in a capacitor is the capacitance, the capacity value, times the square of the voltage. So that's why the breakdown voltage being high is so important. The more voltage you can pressurize this capacitor with, the energy goes up by the square of that voltage pressure. So you want it to be as high as possible.

Okay. So take an existing battery pack that's well known, like the Tesla Roadster. I know that you had someone on the show recently, Leo, who is a Tesla Roadster...

Leo: Yeah, Jason Calacanis. He owns it.

Steve: And loves it.

Leo: And loves it.

Steve: And for people who don't know, this thing is - it can do zero to 60 in, what is it, four seconds?

Leo: Yeah. But this is typical of electric motors. They have huge torque.

Steve: Yes. And so essentially what happens is you are - the electric motor is nearly a dead short. I mean, its own resistance is so low. And so you just - you take this huge lithium-ion battery pack, which has been charged up, and you dump its power as quickly as you can across this electric motor, and it just kicks you, literally, into high gear. Okay. The...

Leo: Tony, who edits the show and is sitting in the other room and is a fan buff, as is Colleen - a car buff, as is Colleen, says you get maximum torque at 1 rpm.

Steve: Wow.

Leo: So that's, like, right away, basically; right?

Steve: Yes, instantly. Like from a dead stop.

Leo: Yeah. Amazing.

Steve: The Tesla Roadster can go about 240 miles on its battery pack. And it stores about 52 kilowatt hours is the amount of storage, 52 kilowatt hours. So that's - a kilowatt hour, or a watt hour, is a measure of energy because it's an amount of power times time. So it's like, for example, 52 kilowatt hours would be 52,000 watts for one hour, or one watt, 52,000 hours, or any ratio in between. So it's a measure of energy storage.

Well, the patent is linked on the show notes page. Every detail, I think it's an 11-page patent that describes in detail the manufacturing procedure and the composition of what these guys have done. They have created, essentially, an ultracapacitor that is substantially more dense than lithium-ion in terms of its energy density. It weighs less. It's about - I think it's about half or less, a little less than half of the volume, yet stores the same amount of power. They talk about this prototype being 300 pounds and occupying about 2.6 cubic feet and storing the same 52 kilowatt hours of energy that the Tesla Roadster lithium-ion pack does. But because it's a capacitor, it first of all has no toxic substances at all, no hazardous material. If you have enough power to charge it, you can charge it in five or six seconds.

Leo: There is an issue, though, that you can't plug it into your wall and charge it in

five or six seconds.

Steve: Correct. So...

Leo: You don't have enough juice.

Steve: So what this is, this is a 31-farad capacitor.

Leo: Wow.

Steve: 31 farad.

Leo: Not microfarads.

Steve: Right. So think of it for...

Leo: What the heck?

Steve: If we put it in terms of microfarads, it would be 31 million microfarads.

Leo: Jiminy.

Steve: And...

Leo: So we're talking a signif- I mean, like, many orders, a thousand orders of magnitude improvement here.

Steve: Yes. 31 million microfarads at a breakdown voltage of about 5,000 volts. They run it at 3,500 volts. So they've, again, got some headroom. But so remember that the energy storage goes up with the square of the voltage. So the key is to run these ultracapacitors, if you want ultracapacitors for energy storage, they want to have the highest possible breakdown voltage. But we mentioned charging them up. Okay. To charge this 31 million microfarad capacitor, or 31 farad capacitor, up to 3,500 volts, and let's say we gave it five minutes.

Leo: You need a power plant. You need a nuclear power plant in your backyard.

Steve: Well, 360 amps.

Leo: Okay. And the typical house has, what, 20.

Steve: Well, yeah. A 15- or a 20-amp circuit.

Leo: Right.

Steve: And so, for example, that would take about 30 hours.

Leo: Okay. But there are talks of, like, you could have another capacitor that you're trickle-charging.

Steve: Exactly. You would have one that sits there charging.

Leo: Like a reservoir.

Steve: The cool thing is that you would charge this at night when the electric power rates are lower.

Leo: Cheap, yeah. This is actually something people talk about. If everybody bought Teslas, there'd be this sudden drain on the electricity. You need this kind of capability of spreading it out to non-peak hours.

Steve: Well, and in fact I think Tesla owners end up with, like, specially wired circuits in order to...

Leo: They don't have to. But it's certainly beneficial. It charges faster that way.

Steve: Right. So anyway, I wanted to bring this to people's attention. This relates - oh, also they have cycled, and this is in the patent, they have cycled one of these - I should mention that anyone who's interested can read the patent. It's actually made up of almost 32,000 small subunits. So it's through an integrated circuit-style printing technology.

Leo: Oh, interesting. So very cheap.

Steve: Yes. And...

Leo: Ultimately.

Steve: ...mass producible is their goal. They were certified...

Leo: How big are they, though? I mean, how - are they giant?

Steve: Well, no. I mean, it's like a third the size of the equivalent lithium-ion pack. So you could have two of these in a Tesla Roadster and get 500 miles. And as I understand it, I haven't done the math, but I think it's like, at 20 cents per kilowatt hour, it takes $10 to charge it up. And you get 240 miles out of it.

Leo: Unbelievable.

Steve: Well, the other thing that is interesting is now scale this down. This changes cell phones and laptops. I mean, now you don't mind that the Air, the Apple Air, has a nonremovable battery. Doesn't have a chemical battery at all. It's got a supercap in it. And you plug it into the wall, count to five, and pull it out. I mean, it's the way it should be. And, oh, what I mentioned was, in the lab they cycled their ultracap, one of the smaller subcomponents, because it's all built up out of little cubes, and they have diagrams and show this in the patent, they've cycled it a million times...

Leo: Wow.

Steve: ...and then remeasured it for capacity and leakage and various other physical properties. No change.

Leo: So this stuff doesn't degrade.

Steve: It never degrades.

Leo: Doesn't wear out.

Steve: There's nothing there to wear out, Leo. It's ceramic separating plates that have been printed...

Leo: This is huge.

Steve: ...and bound together. It's why I'm so excited about it. Oh, and self-discharge. Self-discharge is a problem with all regular electrochemical batteries. They tend...

Leo: They leak.

Steve: Normal batteries will discharge, like, 10 percent per month, for example. This is 0.1 percent per month.

Leo: So you could charge it up, and a year later get in, and it's all there.

Steve: Yes.

Leo: Wow.

Steve: Yes.

Leo: Now, they have an exclusive deal with a company called Zenn, out of Toronto.

Steve: Zenn is a Canadian car company, a strange little car manufacturer. I, for the life of me, I don't know why they would sign an exclusive deal with anybody. Zenn gave them some money. Kleiner Perkins gave them $3 million. I mean, if I had $3 million I would have given them $3 million. I mean...

Leo: This sounds like something that'd be worth investing in.

Steve: Yes. The problem is, though...

Leo: Production.

Steve: ...that they're not the only game in town. I mentioned Georgia Tech is working on this. BASF has a patent on barium titanium oxide capacitors. So we know that - and you cannot patent a capacitor. So there may be other useful ways to build an ultracapacitor. What has got me so animated is that here's one. I mean, this thing, if you read the patent, and you believe their claims, they're in production soon. And we're going to be seeing cars that have removed the problem of lithium-ion battery packs. It no longer dies after a few years. You can charge it as fast as your electrical supply will because it'll just suck in energy at the maximum possible speed. And you can imagine why Lockheed-Martin is interested, too, because capacitors will give up all their charge immediately. So you could imagine some sort of space-based lord knows what, charging with solar cells and just waiting to dump the ultracapacitors into some sort of beam weapon and just punch a hole in whatever it's aimed at.

Leo: This is amazing.

Steve: It is really cool technology. And it also is important for solar and wind.

Leo: Oh, yeah.

Steve: Because the problem with solar and wind is that they are non-uniform. You only get solar power when the sun's shining on it. You only get wind when the wind is spinning the turbine. And so you want some way, some economical means of storing that power for use when you don't have raw input coming in. And the problem is lithium-ion cells have all the downsides to them. Ultracapacitors have none of them.

Leo: Now, we should point out that this is just a patent. They haven't shown they can produce this thing. They actually haven't even tested it. I mean, the Patent Office doesn't verify the claims.

Steve: Right. They can claim anything they want to.

Leo: Yeah. Zenn believes that they'll be producing a car this year based on this.

Steve: Right. Right.

Leo: I would buy that car in a minute. You know there's a Zenn dealer down the street from here.

Steve: No kidding.

Leo: Yeah. In Petaluma. I would buy that car in a heartbeat.

Steve: My feeling is this is the future. I mean, I read an article a couple weeks ago saying that I think it was Toyota was going to build a lithium-ion battery plant in the United States. And I'm thinking, stop. Why bother? Build an ultracapacitor plant. I mean, it is so clearly the right solution.

Leo: Unbelievable.

Steve: Yeah.

Leo: And I tell you, I mean, what I can see people doing is generating solar electricity. And now you have a very efficient storage medium for that, really could change everything. I mean...

Steve: Well, and in fact I was talking to Mark Thompson, my buddy in Phoenix. He was talking about in regions where the daytime power cost is so much higher than the nighttime, you could imagine people getting an ultracapacitor and charging it up at night

and then using the power during the day. Which the power companies would love because they have a hard time delivering power at peak demand.

Leo: Right. They'd like to spread it out themselves.

Steve: Yeah.

Leo: Well, I'm sure when the first person said I've got this thing called a microprocessor, that people laughed and scoffed. And some people, maybe somebody like Steve Gibson, said that's going to change everything. This is, I think, on that order of magnitude.

Steve: I do, too.

Leo: And boy, I hope it's real. That's exciting. That's real exciting.

Steve: Well, these guys who founded the place are from IBM, a senior manager of disk-storage technology, and Xerox PARC.

Leo: Okay.

Steve: I mean, these are not fly-by-night con artist people. And Kleiner Perkins is not known for wasting their money.

Leo: Yeah. It's pretty credible.

Steve: I just - it was such a cool thing, the patent was just granted, all the details are there, linked from our show notes for this episode. I just wanted to cue our listeners in and let them know that this had happened because I think it is potentially big news.

Leo: Very exciting. Very exciting. Steve Gibson, you as always bring us great stuff. Normally security stuff, but today two very interesting stories that don't have a security angle on it. Next week we'll go back to doing our Q&A, our regular Q&A.

Steve: Yep, go back to our original phase.

Leo: And we mentioned at the beginning of the show you can go to GRC.com and get all the information. Steve's made a special SnipURL for you, snipurl.com/sn177. That's the number of this show. Or just go to GRC.com/securitynow, and you'll find it there. You'll also find 16KB versions of the show, if you want to share this with somebody else, our special two-hour 2009 edition. You can also get show notes

there, transcriptions if you'd like to read along, and Steve's great stuff, including SpinRite. You didn't do a SpinRite letter today.

Steve: I didn't. I have one right here in front of me from Officer Greg.

Leo: I'd like to hear it. Officer Greg.

Steve: Well, I got a kick out of it. He titled it "SpinRite Beats the Police." And he said, "Greetings, Steve. I just wanted to share my recent experience with SpinRite with you. I am a police investigator for a medium-sized metropolitan police department in Southern California." So somewhere down here in my neck of the woods. He said, "My partner Detective Rick and I are both avid photographers..." - you'll relate to this, Leo. He says, "...in our off time, and both exclusively shoot high megapixel digital SLR cameras. Since convincing him to make the digital SLR switch, I've stressed the importance of backing up his image storage drives. He has always assured me that he was. Turns out he was just telling me he was backing up to get me off his back."

Leo: Get him off his back. Oh, that's terrible. Ooh.

Steve: So he says, "A few weeks ago the inevitable happened. His hard drive crashed. Thousands of images were lost. Detective Rick was devastated, and his wife was PO'd." He said, "I immediately volunteered to try to save the drive for him using SpinRite. Unfortunately, Detective Rick didn't believe that a single program could help. Instead, he took the hard drive to our local computer forensic evidence experts. After two days our forensic investigator only managed to recover a few files and declared the drive dead."

Leo: Oh, dear.

Steve: "Convinced he now had nothing left to lose, Detective Rick turned the drive over to me. I took the drive home and let SpinRite have a go. Two weeks later SpinRite finished its run. I took the drive back to Detective Rick, along with all of his image files. He promptly moved the data over to two new drives. Now he's a firm believer in backups." So he says, "He moved the data over to two new drives and bought my lunches..." - and says, parens, "(and now he's a firm believer in backups) and bought my lunches for the next week. Our computer forensic unit, after seeing the results, plans on purchasing a copy for their toolkit. I run SpinRite on all my drives quarterly for maintenance, and proselytize its virtues to all that I can. Thank you for providing a great program, and keep up the good works. Once again, SpinRite saves the day. Officer Greg."

Leo: I love the variety of people who use SpinRite. It's really neat. That's wonderful. SpinRite is available at GRC.com. That's the place to go, the Gibson Research Corporation. And lots of other great free stuff there, too. Try out some of his free stuff. Steve, Happy New Year. Happy 2009. Our first show of the new year completed.

Steve: Yup. We've got a ton of Q&A stuff built up from our weeks of prerecording. So we will be back doing Q&A next week for Q&A #57, Episode 178. And I will say again, anyone who thinks they are interested in this PDP-8 opportunity, it is truly once in a lifetime. Bob, I'm glad he's willing to do this again. And it's only enabled by him having a bunch of these Harris HD-6120 chips. You can get the PDF for the chip itself and take a look at the chip and the instruction set and all that on his site. And I think a bunch of us are going to have PDP-8s, which is going to be very cool.

Leo: Very cool, indeed. Thank you, Steve. Happy New Year. We'll see you next week on Security Now!.