SECURITY NOW!

Transcript of Episode #243

State Subversion of SSL

Description: Steve and Leo catch up with the weekly security news, and Steve shares his very positive impressions of his Apple iPad. Then Steve explains why and how world governments are able to legally compel their national SSL Certificate Authorities to issue Intermediate CA certificates which allow agencies of those governments to surreptitiously intercept, decrypt, and monitor secured SSL connections of any and all kinds.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-243.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-243-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 243 for April 8, 2010: Subverted SSL.

It's time for Security Now!, the show that's covering all your security needs, online and off; privacy, too. Well, we don't talk about it. Actually we could. I don't see any reason why we wouldn't talk about lock-picking, but we haven't done it yet. With us right now the King of Security, our man in charge, Mr. Steve Gibson, the guy at GRC, the Gibson Research Corp., GRC.com, creator of SpinRite, world's finest hard drive and maintenance utility, and also many other free utilities. And he's here to help us understand why everything's so messed up. Hello, Steve.

Steve Gibson: It's funny you mentioned lock-picking because there was a lock that I ran across just the other day that I seriously considered bringing up in Security Now!. It's the amazing new Master Lock which is user programmable. And you can set your own combination of any length that you want. And I thought, okay, wait a minute. How are they doing this? It's a hash.

Leo: Oh, clever.

Steve: It's a mechanical hash. And of course we know all about hashing and how you can, by the nature of a hash, you're able to reduce a document of any length into a resulting hash. Well, the Master Lock people - and I'm sure this thing's got patents till next, you know, till the next decade or century - they came up with a way of creating a mechanical hash of a combination that you put in. So you run through the sequence that you want to use to open the lock. And then you say, I'm done. And that leaves the whole bunch of little wacky wheels in a certain pattern.

And then subsequently, when it comes to unlock the lock, if you are able to duplicate exactly that set of sequences - oh, and it uses just a simple up, down, left, right, like a little joystick thing on the front. So it's like, up up down, left left right left, up down, like whatever sequence you want. And it essentially memorizes that, but it doesn't do it like memorizing every action you took because I don't know how you'd do that mechanically. Instead, it ends up building a hash out of your actions so that, if you're able to repeat them, you'll get the same result, and the lock will open. So...

Leo: That's very cool.

Steve: So I have just presented it.

Leo: You see? You see? I knew it. Well, it's funny...

Steve: Thanks for bringing it up.

Leo: ...because when you go to something like the Black Hat conferences or DefCon or HOPE, there's often lock-picking demonstrations. Hackers love the idea of picking locks for some reason. So I guess it was just a matter of time.

Steve: And it's not that hard. But that's another - that's a story for another episode.

Leo: Another matter. Yeah, maybe we don't want to get into that. So what are we doing today?

Steve: We're going to talk - we were going to be continuing our series on how computers work.

Leo: Okay.

Steve: But a paper, an academic paper got published by a couple of young Ph.D.s, actually one's a candidate at the University of Indiana, describing their rather distressing discovery that SSL and /TLS, Transport Layer Security and Secure Sockets Layer, is unfortunately not guaranteeing that we're not being eavesdropped on, which is one of the fundamental benefits of using SSL technology. We've talked about it many times in different contexts, how thanks to the nature of the so-called PKI, the Public Key Infrastructure, where a Certificate Authority signs a web server's certificate, which the web server sends to our browser when we browse to that site, we're able to rely upon the fact that we're really at the site that we believe we are, so that provides authentication, and the fact that we have established a unhackable, impenetrable, uneavesdroppable, encrypted secure connection between our browser and that web server. Well, it turns out that none of those things are true.

Leo: Oh.

Steve: So we're going to discuss this rather distressing bit of news.

Leo: Oh, dear.

Steve: Yeah.

Leo: Subversion of the SSL infrastructure, our topic today on Security Now!. We also have some security news we want to get to in just a little bit, and errata. And I know you have an iPad, so I'm very curious what you think about it. I don't know if we're ready to talk about the security of the iPad. But we can certainly talk about the iPad as a Kindle replacement because you're a big Kindle fan.

Steve: Well, and the fact is, I've gotten - I've gotten. Where did all the vocabulary go? I've received a great deal of email from our listeners, saying, so, what do you think? And I said, well, we'll cover that on Security Now!, so...

Leo: Absolutely. So do we have errata before we...

Steve: We do, well, we've got security news. Pretty much the standard lineup of folks. Firefox surprised the world, however, by already updating again since last week, when we talked about the upgrade to or the update to 3.6.2, which happened at the end of March. Five days later they were again at 3.6.3. Now, I'm glad that they have this policy. I think it's increasingly clear that the Microsoft and second Tuesday of the month updating policy is beginning to fail in light of the evolving threat model that we're seeing where attacks are becoming more and more targeted. It means that you really can't wait 30 days to have these things fixed. So I'm pleased that the Mozilla folks maintaining Firefox, when they find a problem that is sufficiently troublesome, they don't care if they did it five days ago. They fix it immediately and push out an update.

Leo: I think that's kind of the accepted norm in open source software. There's just no - you don't hold back. You get it out the minute you've got a fix.

Steve: Yeah. Well, and so they have. They have a memory corruption flaw that could be exploited to inject and execute malicious code provided by the attacker. So that's as bad as it gets. One of the standard, send you a link in email, and if you're using Firefox your machine is owned, as they say. They also took the opportunity, I thought was kind of cool, to fix a problem that's sort of floated around the 'Net. It's considered an information leak vulnerability, and you've probably run across it before. I don't think we've talked about it, Leo. And that is, there was a way that websites could learn where you had been before because web browsers, as we know, color visited links differently than never-visited links.

Leo: Right.

Steve: And so there was a way that, using scripting, a website could present some links and learn what color they were on your browser page and obtain that information back to the web server. So the problem was they hadn't - this had been sort of lurking as a known kind of, oh, well, that's kind of not so good. I mean, it's not like a horrible problem, but still you'd like to keep that information to yourself and not have sites you visit have any way of knowing what your habits are and where you may have visited before. So that they fixed, finally. They came up with a way of fixing it that didn't break other things, which is what had kept them from doing anything about it until now. So that also got fixed with v3.6.3, which is where we are now with Firefox. That is, as of the date of this recording. It may be stale soon. But...

Leo: Who knows, yeah.

Steve: That's more power to them. I noted on one of my machines that the Java Runtime Environment was telling me that it needed to update. And so I wanted to advise our listeners of that, to look in their tray. Normally, if you've got the so-called JRE, the Java Runtime Environment, installed, it will - it's keeping track and looking for updates. It was a relatively important update.

Just reading from the SANS Institute summary, they said, "Sun's Java Runtime Environment, a virtual machine environment that operates on many platforms, is prone to multiple remote code execution vulnerabilities. Two buffer flow vulnerabilities exist in Java's handling of midi sound banks. In addition, an input validation error exists in the processing of certain image files. All of these vulnerabilities can be exploited by enticing the user to visit a web page containing a malicious applet" - that would be a Java applet - "and accompanying data files. Various other vulnerabilities in the JRE have also been reported and patched. Some technical details for these vulnerabilities are publicly available."

So my sense is it's not super widely used. Normally what happens is you'll download some application which says it's written in Java, so you need to install the JRE, the Java Runtime Environment from Sun, on your machine. So I wanted to let our listeners know about that. So check to see if that's happening. Now, one thing...

Leo: I think my Mac did update, as a matter of fact. I think I remember, yeah.

Steve: Yeah. One thing that did not automatically notify me, so I'm glad I checked, is QuickTime on the various Windows platforms. Apple put out an update of their Windows version of QuickTime, bringing us to version 7.6.6. And so that's on both XP Service Pack 2, Vista, and Windows 7, the three current Windows platforms. And this fixes a bunch of different sort of standard code execution vulnerabilities involving the display of PCT or BMP images, or even a malicious video could be created that would trip this vulnerability. So that you don't get an automatic update for.

So what I did was I launched QuickTime myself. And then I think when I ran it, it did do an automatic check and said, oh, there's a new version. And so I said, oh, good, I want that, and downloaded it. It's big. It's 38MB. It took a while. But it's worth doing because the problem would be you might click on a link to a QuickTime video, an MP4, whatever you've got that's associated with QuickTime in email, which would launch the player and could cause a problem for your system.

And then the most interesting problem is, turns out not to be a vulnerability, but a hack that a very PDF-wise developer named Didier Stevens came up with. It turns out that Adobe PDFs, by design, are able to launch other system applications, that is, other system executables in order to display content embedded in the PDF.

Leo: That doesn't seem right.

Steve: It doesn't.

Leo: I guess that's like a browser; right?

Steve: Sort of, yeah. So the idea, well, the idea would be you might have an embedded data file like, I don't know, an Office document or, I mean, anything, which needs another app in order to view it. And so by definition, by design, the PDF format allows the embedding of foreign content, displayable with third-party apps. Well, not surprisingly, there's a way to exploit that. This guy, when you do this, you do get a dialogue box asking for permission to run the app. What Didier figured out was a way of manipulating the messages that's displayed in that dialogue box, so to use some social engineer in order to induce people to do it.

For example, and he shows this on his page, he shows a sample permission dialogue where it says - he's replaced the normal text with "To view the encrypted message in this PDF document, select 'Do not show this message again' and click the Open button." Well, so if a user did that, they would be instructing Acrobat to not ever present this interception dialogue again, giving it free rein in the future to automatically run whatever program you want. And it turns out he's figured out a way to run arbitrary code, essentially. So he could bundle his own malicious code and get this thing to run it. The good news is - oh, and I forgot to mention that because this is part of the PDF spec, other readers, like the Foxit Reader, are similarly vulnerable.

Leo: Oh, interesting.

Steve: Because they followed the spec. And so they had to put this feature in. So the good news is - now, we've told people before, our listeners, about disabling JavaScript in Acrobat. If you open up your Acrobat Reader, your Adobe Reader, under the Edit menu at the bottom is Preferences..., which opens a large preferences dialogue with a whole list of categories down the left-hand side. Our listeners will have already selected the JavaScript category, and the first checkbox there is Enable Acrobat JavaScript. Hopefully that's already been turned off by them because you just don't want that. We've talked about how rare it is that PDFs require scripting. Mostly you're just looking at static documents.

Further down the list - that list is alphabetically sorted - down toward the bottom you want to go to Trust Manager. So choose Trust Manager over in the left-hand column. And again, at the top of the right-hand side you'll see a checkbox, "Allow opening of non-PDF file attachments with external applications." Unfortunately, as is the case with JavaScript, it is enabled by default. So turn that off if you do not want this functionality. And I would advise people to do so. So what this does is it just says that you're no longer allowing Reader to essentially get exploited in this fashion. What this creates is the possibility of malicious PDFs that aren't taking advantage of a flaw that Adobe or Foxit or anybody else displaying PDFs needs to fix, but rather taking advantage of a feature that's there by default but which security-conscious people almost certainly don't want to have. And with the disabled it is - what you get is a popup telling you that something is trying to run an external program, that is, you know, this document is trying to launch an external program, but you have disabled that in the Trust Manager. So it's not like you lose any functionality. You get the warning, which is probably, well, we know is a very good thing. And it prevents this from executing in any case.

Now, Didier has a demo of this on his page. And I will post the link on the Security Now! site for our listeners. You can post it in the show notes. It's just blog.didierstevens.com and a URL there that I won't try to do verbally. But on that page, and this page is where he goes into detail and explains this, but down toward the bottom he has provided a demo PDF, which is very cool, which is like a K big, so it's very small. And it just allows you to safely test your Acrobat reader to - like in both settings. And I've played with it on and off and verified that it does the right thing.

So it's just a nice little test that Didier - he has not disclosed, he has released as a proof of concept the ability to overwrite the text in the dialogue box. His sample PDF does not do that. He has not released that publicly. Because that's really the danger that allows the social engineering hack to trick people into saying, oh, I guess I have to press Okay, actually Open, in order to proceed, which would then compromise their machine. However, he's provided this information to Adobe and Foxit so that they can fix these problems. And there will be an update to that because you should not be able to override the text in this dialogue, which is really the trick that he came up with. But in the process it disclosed something that security-conscious people would absolutely want to disable in their PDF readers.

Leo: And he does have a fix for it. In fact, he's got an update on his blog, I just, I noticed to the whole thing.

Steve: Well, there's additional information because Adobe and Foxit have moved on this problem. And there's a sort of a complicated logic sequence he goes through because Adobe, or rather Foxit had some sort of a problem that required a second type of exploit in order to make it behave the way it did, meaning that it really wasn't - there was always a bug in Foxit the way it was. And when they fixed it, they cured the bug, but then they caused another problem or something. So anyway, the point being, this is something our listeners ought to have turned off, just like JavaScript, because who knows if this will be the last problem we see this arise. Many times we see, well, for example, JavaScript hacks perpetually, essentially, in PDF files. Well, just turn it off, and then you've got blanket protection.

Leo: All right, Steve. You and I both got our iPad. Now, I think you had a UPS delivery issue, didn't you? What happened there?

Steve: Well, the saga began with me expecting the iPad, as everyone did, to arrive on April 3rd. And so it turns out that it's possible from Apple to download and print a delivery release, which I did, and had it stuck on the front door so that if, no matter what happened, if I somehow didn't hear the doorbell, or I was in the shower or, you know, on the phone or something, that the UPS guy would leave the box. So it was after you got yours, because I was watching you on KFI, The Tech Guy, on Saturday, and saw that...

Leo: I got it, like, 10:30 in the morning, I think...

Steve: ...you know, with longing, yes, the delivery of your four.

Leo: That was so fun.

Steve: Your four iPads.

Leo: Yes.

Steve: And so I heard a knock at the door maybe at about 11:00. And went to the door, and the guy was pulling the waiver down off the door. And I thought, oh, okay. He was holding a box that was substantially too small. And I looked, and it was Amazon. And it's like, oh. And I said, "Where's my iPad?" And he looked at me and says, "Oh, you've got one of those, too?" I said, "Yes." I said, "I'll trade you the Amazon box. No matter what it is." And he said, "Oh, hold on a second." So he goes down to his big brown UPS truck, and he spent a long time down there. And he came back empty-handed. It's like, oh. So, you know, my world just collapses.

Leo: Aw.

Steve: And then I realized that he was not maybe, well, he wasn't my regular driver. He didn't seem to be dealing with, you know, a full deck of cards because he was taking the signed release down for the wrong box. It was, you know, it was a release for the iPad, not for the Amazon. Amazon doesn't require that. So I'm thinking, okay. And so he says, "Oh, it's probably on another truck." Well, there's never been more than one truck. And I said, "What?" And he said, "Oh, yeah, there'll be another truck along." And it's like, okay. I'm thinking, I hope you know what you're talking about. So...

Leo: I think they did Saturday deliveries.

Steve: Well, he wandered off. And I thought about this for about a half an hour, and I thought, okay, I've got to find out what's going on. So I found a number for UPS and got the robot that said, "Would you like to track a package, ship a package, or...." There were three choices, none of which I wanted. But I said "Track a package." And so then I spoke my tracking number in clearly, and it told me that it was in transit. And the web page is supposed to say "out for delivery" when it's actually coming to you, but it didn't. It kind of got stuck at 7:30 saying "arrival status" or something. So then, so the little robot says, you know, "What would you like to do?" And it gave me my three bad choices again. And I just, I closed my eyes, and I said, "Talk to a person."

Leo: Ooh.

Steve: And it said, "Just one moment, please."

Leo: It worked.

Steve: I couldn't believe it.

Leo: It understands my - wow.

Steve: So I got a really nice lady who I started to explain the problem, and she was - I heard her sort of sighing.

Leo: She had a few calls like this.

Steve: And I said, "What?" And she says, "I know, I know." I said, "Oh. So you mean this guy could be correct? There might be...." She says, "Trucks are circling your location right now."

Leo: The black helicopters are out.

Steve: I said, "Really." And she says, oh, she said, "This has been an unimaginable day." She said, "Our web system, our IT infrastructure has collapsed under the burden of delivering all these iPads on Saturday."

Leo: Oh, that's interesting. "All these iPads." Wow.

Steve: Oh, yeah. All the trucks are full of iPads and nothing else. They had iPad-only trucks going out. She said, "What's really been upsetting for people is those who ordered multiples often had them on different trucks."

Leo: Oh, dear.

Steve: So the first one would come, and you'd get, you know, Joe Apple Fan Boy would get, you know, one. And he'd say, well, where's my other two? And then the guy would go down and look in the truck again for 15 minutes and come back and say I only have one. It was like, oh. And then, you know, another truck would show up with another one. And then another one would show up. So anyway, it was a - sure enough, a second truck showed up with a box the right size, and I was quite pleased.

Leo: Yay.

Steve: So I spent about two hours with it, poking around, getting a feel for it and liking it a great deal.

Leo: Oh, good.

Steve: I was in the shower thinking about my experience with it, and...

Leo: Not too hard, I hope.

Steve: And suddenly - I wasn't that excited about it, Leo. And suddenly I thought, I really am going to use this all the time. This is, you know, and remember I had prided myself on purchasing the cheapest one because I didn't want, you know, I knew that a year from now we'd get a camera, and other things would be improved. That's what Apple does.

Leo: Right.

Steve: And so, and I knew that this was the one, you know, the 16GB one was the one that Jobs least wanted me to purchase because it was one that made them the least amount of money. Because it certainly isn't costing them a hundred dollars to double the memory and a hundred dollars to double it again. So I thought, okay, fine. This is the most sensical thing to do. But in the shower it occurred to me that this thing was probably going to go crazy when - because it was so good - when the world started to find out about it. So I quickly dried off...

Leo: No.

Steve: ...and ordered the most expensive one.

Leo: For later delivery. You mean the GPS...

Steve: For whenever it comes, whenever it comes.

Leo: Isn't this funny. Because guess what I did, Steve? Exactly the same thing. I got the 64GB with 3G, and that's coming towards the end of the month. Yeah, exactly the same thing.

Steve: So here's my feeling. People who - first of all, it's dangerous to go out in public. I tried to have a quiet dinner by myself on Sunday night.

Leo: Me and my iPad.

Steve: The entire restaurant staff and most of the diners that were within eyesight had to ask me about it and touch it and feel it and so forth. The general consensus is that everyone who has seen it wants one. There's this massive iPad lust. And I'm stunned by the amount of buzz that Apple has created over this. It's just phenomenal. I was annoyed that the store was closed, the Apple store was closed on Sunday, being Easter, because I wanted to get a couple cases for it, and I couldn't wait for the ones that I had already purchased to come in the mail or to be delivered. And I did go up to the store on Monday, and it was still super busy.

The criticism we've heard, well, there's a number of criticisms, of course. One that concerned me at first was the absence of multitasking. But apparently I don't need multitasking because I'm able to do multitasking things sort of by doing one thing at a time. For example, the other day I saw a - I was looking at some blog where there was a photo. I was actually looking for iPad easels because it's clear to me that some sort of a tilt, like a tilt stand is really what you want for this thing. It is heavy. It is substantially heavier than the Kindle. It's not the kind of thing you'd be comfortable holding with one hand. I really think it needs a case or some skinning. In fact, I've ordered the GelaSkin, which I had purchased...

Leo: You love those because you sent me one for the Kindle.

Steve: Yes. And I have them on my Kindles. I like the fact that it's a little bit tacky, meaning that it's - you've got to - it's a much better grip. And I'm just really afraid I'm going to drop the iPad because it's sort of - it's all shiny and smooth and slippery with its brushed back. In fact, the Apple logo, the black Apple logo on the back is sticky. I mean, that's the way I wish the whole thing were. So I'm going to add that back skin to it.

I sort of don't like any kind of a cover. You know, for the Kindle I have a slipcase where I just pull it out, and then it's unencumbered with any flaps or covers or anything else. Although I have to say that Apple's own brand cover is pretty nice. I used that for a couple days. The pad slips in where the hinge is, and then you flip this little flap over and down behind the iPad to kind of lock it in. And it's not - it doesn't add much bulk to it, and it does give you some screen cover protection. I dislike the high gloss. I dislike that on Apple's laptops. I dislike it on any LCD screens. So I'm going to try, I have ordered from a company called iLuv, a matte screen protector to see what happens, just to see how it looks.

Leo: The glare really does become a problem if you're in a brightly lit area. Well, you can see when I hold it up it reflects everything, including my lights, my eyes, you know.

Steve: Oh, you can adjust your eyebrows. I mean, if you want a mirror, you've got one built in. Just turn it off, and it becomes a mirror. And of course it is absolutely a fingerprint magnet. I decided, well, rather than wiping it down all the time, I'm going to understand that it's meant to be touched. And so hands have oil on them, and it's just going to - I'm just going to look through the fingerprints and not be annoyed by that because...

Leo: You don't see it so much when it's on. I keep a little swaddling cloth in my - you know, a little microfiber cloth in my case.

Steve: Right.

Leo: So I can wipe it off. But, you know, you don't see it when it's on. It's only when it's off that you really notice the thing is all smudged up.

Steve: So my two dreams, and I think I've stated this on the podcast before, I've got every gadget under the sun. I love my BlackBerry for messaging, real-time connectivity. I've gotten pretty good with the little keyboard. I've got the Tour, which is the 480x360, or maybe 320, resolution screen, the same resolution as on the iPhone and the iPod Touch. It's a smaller physical size, but the same pixel count. So, yeah, you could surf the 'Net if you had to. But it's not pleasant. I mean, it's really cumbersome to do that.

So what I wanted was the ability to, wherever I was, quickly jump on the 'Net. And I have got laptops. I've got any laptop I want. And but the laptop you've got to get it out of the case, open it up, turn it on, in my case wait for Windows to boot, which isn't ever fast. And even if you do a restore from having it hibernated, that still takes substantial time, I mean, enough so that it's not conducive to just doing short-term web browsing. So that dream is absolutely answered with the iPad. In fact, I'm really impressed with the way they manage WiFi connectivity already. When I go into a Starbucks or into somewhere with an open WiFi hotspot, and when I turn it on, it already shows that it's connected to that location. I mean...

Leo: Right. Oh, it does open automatically.

Steve: Yeah.

Leo: Interesting.

Steve: I'm very impressed. And if I left the web browser as the last thing I was using when it turned it off, it's back at the web browser. So, I mean, as, like, a dedicated browser, I've got my dream come true. I mean, it's an instant on, no boot, I'm in a web browser and ready to go. The second thing I've always wanted is a really practical PDF reader. Yes, the Kindle DX can read PDFs. But one of the things you really feel from using the iPad, having been a Kindle user, is when you then go back to the Kindle, oh, what is taking it so long?

Leo: It's a very slow device.

Steve: The Kindle is so slow. Now, of course, the reason it's slow is that it's running its processor very slowly because we know that the faster you go, the more power you burn. And the Kindle's great advantage, coupled with its lack of speed with the iInk or the eInk display, is the battery lasts for weeks. On the other hand, the iPad, as we know now from the reviewers who played movies from 7:30 in the morning until 7:45 in the evening, 12-plus hours of constant use, the battery has ceased to be a problem.

Leo: Isn't it amazing?

Steve: And I absolutely feel that.

Leo: I'd love to know how they did that.

Steve: I've also, I mean, they really solved that problem. So, and I think I felt a little breath of hot air come out of the docking connector yesterday, Leo.

Leo: Oh, interesting.

Steve: It's interesting because there's no obvious ventilation. But I kind of - I think it kind of exhaled on my hand because my hand was near the docking connector. And I'm sure I felt kind of a [breath].

Leo: I haven't felt any heat at all. And so that's interesting.

Steve: No, yes, I haven't either. Until that one moment where the back of my hand happened to be by the docking connector, and I think it kind of exhaled heat onto my hand. So I'll be interested to see if anyone ever experiences that. But there is, first of all, the iPad itself is able to read PDFs natively, so that if you had a PDF in an email attachment, you could...

Leo: Oh, I didn't know that. Oh, that's nice.

Steve: It'll do that. But there is a fantastic reader called Good Reader, should be called Unbelievably Great Reader.

Leo: Really. I bought it, but I haven't done much with it.

Steve: It's a complete library. So one of the other criticisms that, I mean, that I feel is that the iPhone - first the iPod was an appliance of iTunes, that is, typically of a Mac, but also with Windows. Mostly you did your work in the PC or the Mac in iTunes, and then you plugged the iPod in and synchronized it to have all of your - that's the way you got photos into it, and music, and you organized things in albums and all that. So it was sort of a peripheral. Then they upped the ante by doing the same model with the iPhone and the iPod Touch. And again, it was basically slaved to an instance of iTunes running on a machine.

So that approach is still the way you work, largely, with the iPad. And my feeling is, I mean, I'm getting more comfortable with it. I mean, I should explain to everybody, I am in love with this iPad. I think they've hit another grand slam. And I wasn't fan boy. I was skeptical. I bought it, and the cheapest one, because I figured, well, I have to have it, have to play with it, see what I think. I mean, it will be a constant companion from now on. And it's just I couldn't be more pleased with it. But...

Leo: Now the negatives. Do you have any negatives?

Steve: Well, there's a complaint, and this is sort of what I feel is that this - I'm not sure that the model of it as a peripheral of iTunes isn't being stretched a little too much. That is, we want it to be a computer. It almost is a computer. And, for example, it doesn't have a file system. You're not able to manage files on it.

Now, companies have worked around this. And, for example, this Good Reader has worked around it by managing the PDFs that you give to it internally itself. And it does a beautiful job of it. It also has all these ways of getting PDFs into it. It can set up - it can be a server on your WiFi network, allowing you to send it PDFs. You can browse with its own browser websites and download PDFs from web pages into it. You can give it the URLs of PDFs that are anywhere on the 'Net, and it will grab them for you. So they did, they've solved a lot of this sort of themselves.

But mostly, I mean, everything you could want, you could resize the PDF. It does a good job with both portrait and landscape. You can lock - you could, like, size it so that it's column to column, and then there's a little option to lock it so that it won't slide from side to side, but only goes up and down. It's just - that's the second thing I wanted, to be able to really read PDFs easily on a portable device, and I have that.

I love that the iPad has a rotation lock because I'm generally liking it much more in a horizontal, that is, in a landscape orientation than in a portrait orientation. That's generally the way I'm liking it. So I just have it locked that way so it's not starting up the wrong way and then having to swing itself around. So I really like that a lot.

I do think that it is a little bit of an a la carte come-on from Apple. I mean, people are going to be buying a lot of the extras and paying a lot more money for them, like the dock and the keyboard and the camera connector and all - and even the case is $40, which you really do want. Or maybe it's $29.95. You really want some sort of a case for this thing to protect it.

One of the interesting little easels is part of their Apple, or I guess maybe it's Insight, or it's one of the people that they have in their store, sells sort of a silicon wrapper for it. But it's just - and they provide a little stand. It's just a flat piece of plastic with notches at either end, sort of like a ruler that bends. And you bend it and then stick the tablet into the notches. And it does a very credible job of standing it up at a very nice viewing angle. So I like that a lot.

The iBook store has a very weak book selection at the moment. Nothing that I'm reading...

Leo: No, it's terrible.

Steve: ...is available there. So it's like, okay, well, we'll wait for that. But the Kindle reader, I mean, I'm reading my Kindle books as I was on the Kindle, now over on the iPad.

Leo: And they look good. They look very readable.

Steve: They're very readable. I mean, I would say there's no comparison. The readability is vastly superior on the iPad, both because of the size of the screen and the fact that you've got much higher contrast with a backlit white screen with black, black type. The eInk on the Kindle is light gray on darker gray. So my feeling about the Kindle is that it really has not been replaced. I have, because I have one, I still use it.

Apparently The New York Times is going to be coming out with a dedicated app for reading The New York Times. I'll be interested to see that because that's the newspaper that I've really fallen for over The Wall Street Journal and the L.A. Times, all of which I also subscribe to. But I like the - the news stories seem much richer and much deeper on The New York Times than in other papers, as if the writers really know what they're talking about. So I'm glad that there will be that option. But I can hold the Kindle, I mean, yeah, my Kindle 2 in one hand and chopsticks in the other.

Leo: Yeah, you can't really do that.

Steve: You really can't. You cannot hold the iPad with one hand. So...

Leo: Although it weighs less than a hardcover book. I mean, people routinely read hardcover books. So it's not like...

Steve: Yeah, but it's weighty, and a hardcover book isn't quite as large, that is, the moment of twist on your hand holding it is greater with the iPad.

Leo: Yeah.

Steve: It really has...

Leo: You need to rest it on something. You pretty much have to, yeah.

Steve: You do. Which, again, we've got a glass screen. We want it to be this size. I mean, the size being - the criticism among the tech people is that it's just a larger iPhone. It's like, well, yes. But that's a huge difference.

Leo: It's a lot, yeah.

Steve: That makes all the difference in terms of actually being able to surf. And, oh, Leo, the mail app is beautiful. In landscape mode you've got an inbox on the left, plenty of room to read email. I mean, I'd much rather, and do now, read my mail on it rather than on my BlackBerry.

Leo: How about answering? Oh, yeah, it's better than the BlackBerry. But how about answering it? Do you find it typeable?

Steve: Yeah, I'm - I completely agree with the critics who say, or just the reviewers, that this is not a content-creation device.

Leo: Right.

Steve: I think that's completely correct. This is a - it's a content-consumption device. But I want to consume web pages, and I want to consume PDFs, and I want to read my email. And it really does it.

Now, I think there's still a place in the world for the Kindle. But the fact that it's not at retail is going to kill it. The fact that you can't go into a store and compare it side by side to the iPad, I think people just won't buy it, even though it might be a better solution for them. I think they're going to get an iPad. And it's hard to blame them. I mean, the iPad does so much more than the Kindle does. And looks like it's going to do everything the Kindle does and be dramatically more readable. And if the iPad only had a battery life of four hours, I'd say, okay, they screwed that up.

Leo: Right.

Steve: But this thing runs all day. So anyway, I'm completely, completely sold.

Leo: Yeah. Yeah, I have to say I can't put it down. And there are negatives. Look, it's not perfect. And the next generation may add a camera. I don't know if multitask- I find that just the pressing of a button and going to the next application is probably enough for me. I'd love to...

Steve: I completely, yes, I completely agree. I don't know what it is people want in multitasking. I mean, email comes down by itself. Maybe it's Apple's apps multitask, but third-party apps don't? I mean, I'm getting email...

Leo: That's exactly the case. I mean, I can listen to my iPod, play a book, and then go out and continue on with other things while that's playing in the background. So Apple just doesn't let other programs do it.

Steve: Okay.

Leo: And there are rumors that the next generation iPhone software, 4.0, which is going to be announced on Thursday, actually as this show is airing, that it may have multitasking or some form of it built in. And if it does, then that may migrate to the iPad as well, which will presumably run 4.0, so...

Steve: I do have an app recommendation.

Leo: Oh, good.

Steve: I found something I love. I love non-timing-based, take-your-time, combinatorial-style puzzles.

Leo: Me, too. Yes, yes.

Steve: Sliding blocks or...

Leo: Sokoban, that kind of thing, yeah.

Steve: Yeah, or - yeah, Sokoban, or figure out how to create bridges between links and so forth. There is an incredibly inexpensive, I think it's 99 cents, it's called Puzzle Maniak. It has got, I think, maybe 15 different types of puzzles. And it generates them algorithmically, so you never run out of them. You can control the complexity of them. And there are some fantastic puzzles. Like there's just a beautiful map coloring puzzle where you have to color a map with four different colors. And it's just relaxing. There's no one jumping at you, no one shooting at you. You don't have to duck behind rocks. You just - you can stare at this thing, go okay, this has to be green. So you drag a little green over to it. And okay, that means that this has got red and blue and purple on it, then this has to be yellow.

Leo: Oh, I'm buying this right now. That looks fantastic, yeah.

Steve: And there's, like, connect the nodes with the number of links shown, I mean, really interesting, intriguing puzzles that it generates, all kinds of different things. There's one where it gives you a bunch of nodes interconnected by lines. And you just have to - you just drag the nodes around until they're all connected with lines that are not crossing each other. So it's just, I mean, they're - and that's pretty simple. But if you would like to have more nodes, it'll be happy to give you more. And then you just - you spend all day trying to untangle that nest. So I really like Puzzle Maniak. It's, like, perfect for me for the kind of puzzles that I like, are just kind of relaxing, doodle away while you're waiting for something to happen, and you're standing in line or something. Anyway. And it's available for the iPhone, as well, in a slightly reduced size version.

Leo: Great.

Steve: I recommended it to all the people I know who own iPhones because it's, again, just a way, perfect little doodle toy.

Leo: All right. Well, so there's a positive review, and one that actually I concur with for the iPad. I've been really having fun with it. And I think Apple has proven that it did find a new way to make a tablet that might succeed better than what Microsoft has been able to do over the last decade. I mean, they've been - Bill Gates has said everybody will be using a tablet soon. I just don't think he was thinking an Apple tablet.

Steve: I had a note to talk about that, too, because there are people saying, well, sure, but there's going to be 50 other tablets coming out any moment now. And it's like, okay, look. Windows can't do this. I mean, you can't put Windows on a tablet and get the same kind of experience. What you need is a system, and maybe Google's system will do it.

Leo: Android might be a good choice, yeah.

Steve: Yes. But, I mean, you absolutely need something designed for touch from the beginning. You cannot take the assumptions of a mouse-based system and just sort of force them into a touch-based tablet. I mean, Microsoft has sort of tried that with their phone, which has never gotten off the ground until I've heard you and Paul talk about it. They simplified it and basically turned it into their music player, their Zune basically. That UI moved over onto the phone in order to create something that sort of has a hugely compromised, but now finally makes sense, sort of UI, instead of just trying to cram Windows into something that runs on batteries.

Leo: Mm-hmm.

Steve: So I did get a neat note from someone who didn't intend me to read this, so I'm not going to give his name. He's the CEO of a relatively major corporation. He said, "We rent or manage computers that are sent to trade shows all over the world. The PCs are either owned by us or by clients. But we manage them and store them at our offices before sending them out to the trade shows. At the shows, they're used to collect sales lead data and sometimes used as point-of-sale systems. Recently we had a new Panasonic Toughbook fail at a show - a hard drive failure - in Germany, with no way to boot to even a command prompt from USB. We used our copy of SpinRite 6 to recover the data off the drive as a last resort, and it worked perfectly. I'm sure this is no surprise to you, but it was a great relief to us and our client, who had $30,000 worth of orders stored on that machine with no backup. Thanks.

"I'd like to include a SpinRite bootable USB stick as part of a hard drive emergency recovery for every system we ship. We ship about 10 orders per month. They all come back to us after each trade show. Could you please tell me what kind of pricing structure you have to offer. Direct me to the right area on your website. Thanks." Signed, nameless person who's a CEO. So I just, you know, nice little testimonial there about SpinRite helping someone again. And in this case, paying for itself about, well, not a thousand times over, but about, what, 400 times over.

Leo: Well, let's get to the meat of the matter, which is of course today SSL certificates. You sent me a PDF from Microsoft which was updated in November 2009. I guess they update these files, the root certificate files, fairly regularly.

Steve: Well, Microsoft does something odd, which is, if you install Windows fresh, you will only see about a handful, something like 15 root CAs, remember, Certificate Authorities, in what Microsoft Windows calls the Windows Trusted Store. That's where Microsoft stores certificates for the OS. And except for Firefox, the other Windows-hosted browsers, IE and Chrome and Safari, all rely on the Windows Trusted Store.

What happens is, if you go to a website whose web certificate, their SSL certificate is signed by someone not currently in your instance of Windows, Microsoft, it turns out, has a real-time, on-the-fly certificate update facility that works in the background so Windows itself, when the query is made, down in the Windows crypto system, it will see that you're asking about a certificate it doesn't currently have. So it contacts Microsoft and grabs the certificate that you're asking for on the fly. As a consequence of that, we now know that Microsoft trusts a huge number of certificate authorities. And you'll remember, Leo, years ago, when to my horror I looked at the size of my own trust store in Windows, which IE was using, and just said, oh my goodness, I mean, there's so many. Well, turns out there were even many more than that. Microsoft trusts 264.

Leo: Jiminy.

Steve: 264. Now, the fact is...

Leo: Now, are these root certificates?

Steve: These are root certificate authorities.

Leo: Wow.

Steve: 264. Now...

Leo: Including, as we've mentioned before, the Hong Kong Post Office.

Steve: They're there. Apple trusts 166.

Leo: Hmm, I wonder why so many fewer, to be honest?

Steve: Well, just because one wonders about in general Microsoft's tendency towards excess. Obviously people don't have a problem surfing and doing SSL connections from the Mac. So...

Leo: Yeah, they don't need - how many does Firefox come with?

Steve: 144.

Leo: Even fewer.

Steve: Even fewer. And remember that Firefox brings its own CA library with it, even under Windows. So that's another reason why I would give Firefox some props over IE, just for trusting so many fewer CAs.

Leo: Does it supersede? So...

Steve: Yes.

Leo: Oh, interesting. So even though Windows may trust more, it will ignore the additional root certificate authorities when you're surfing with Firefox.

Steve: Well, because Firefox also uses its own crypto library, which it brings with it. There's an acronym for it. It's NSS or NNS. I think it's NSS is the crypto library that the Mozilla group use. And NSS has its own CA store. So since it's using its own crypto stuff, it uses its own certificate pool, as well.

So what happened is, one of the researchers, there's two guys, both at Indiana University, Christopher - I'm afraid about his name here. It's like Soghoian is how I think - S-o-g-h-o-i-a-n, Christopher Soghoian is a Ph.D. candidate in the School of Informatics and Computing at Indiana University. And he's partnered up with Sid Stamm, S-t-a-m-m, who is a Ph.D., also he got his Ph.D. at IU, currently employed by Mozilla. One of them was at a conference where they saw in sort of the trade show portion of the conference a very disturbing booth from a company called Packet Forensics. Packet Forensics was advertising a little turnkey network appliance which was able to perform SSL man-in-the-middle attacks.

Now, we know that SSL man-in-the-middle attacks could be pursued based on the previous problem with SSL where renegotiating sessions had a bit of a hole in them, such that it was possible for a man in the middle to perform some little chicanery, but nothing that was of too much concern. Well, these guys put together a 19-page PDF. If our listeners Google "ssl-mitm.pdf," as in man in the middle, "ssl-mitm.pdf," Google will take you to a bunch of instances of this. It's at files.cloudprivacy.net/ssl-mitm.pdf. You can also find it at cryptome.org/ssl-mitm.pdf.

I'm going to read a couple excerpts from this to explain what the concern is. And then, since our listeners have been so well trained in the nature of browser certificate stuff, I'm going to explain in detail exactly how this appliance can function, and essentially what it means.

So almost taking a chapter from what I had said years ago, they wrote, "While not known to most users, the CAs, that is, the Certificate Authorities, are one of the weakest links in the SSL public key infrastructure, a problem amplified by the fact that the major web browsers trust hundreds of different firms to issue certificates. Each of these firms can be compelled by their national governments to issue a certificate for any particular website that all web browsers will trust without warning. Thus users around the world are put in the position where their browser inherently entrusts their private data indirectly to a large number of governments, both foreign and domestic, whom these individuals would never ordinarily trust."

So to say that another way, or to simplify that, it might be that a given website has purchased its SSL certificate from VeriSign, and our browsers of course all trust VeriSign. Well, to use an example that I've used before, but not to pick on the Hong Kong Post Office, some other agency, for example China, could compel the Hong Kong Post Office Certificate Authority to issue a certificate for, say, Google.com. And we have no way of knowing that that's been done. But it's, from a technical standpoint, nothing at all prohibits any of these 264 random Certificate Authorities from creating a certificate for Google.com. The fact that Google.com actually bought theirs from VeriSign doesn't mean anything to our browsers. All that our browser does, when it's presented with a certificate which it believes is from Google.com, is to see that it's been signed by someone it trusts. Well, it trusts the Hong Kong Post Office.

What this means is that it would be entirely possible for any governmental agency to essentially proxy SSL connections. And if connections are going through some sort of device which is not going to an IP of Google, it just lets them pass. But when it sees that a connection is going to the IP of Google, it proxies that SSL connection, meaning it pretends to be Google, that is, the device does, which it can now do because it has a certificate for Google.com signed by someone our browser trusts. So instead of our connection actually terminating at Google, it terminates at this device.

Our browser gets a certificate from the device, checks to see if it's a trusted - if it's been signed by someone it trusts. It has been because it's been signed, not by VeriSign, but any of a number of these hundreds of certificate authorities, and the browser's happy. Then the device connects to Google.com, and we can't tell the difference.

If we examined the certificate ourselves, we would see, oh, look, it's been signed by the Hong Kong Post Office. That seems suspicious, that Google would have their certificate signed by the Hong Kong Post Office as opposed to maybe VeriSign. I wouldn't be surprised if that's who Google did have their certificate signed by. I haven't looked. But, you know, that's the nature of this problem. But it's much worse, as I will explain in a second. I wanted to read what these guys have done from their research, or said about the nature of compelled assistance.

They say, "Many governments routinely compel companies to assist them with surveillance. Telecommunications carriers and Internet Service Providers are frequently required to violate their customers' privacy, providing the government with email communications, telephone calls, search engine records, financial transactions, and geolocation information. In the United States, the legal statutes defining the range of entities that can be compelled to assist in electronic surveillance by law enforcement and foreign intelligence investigators are remarkably broad. Examples of compelled assistance using these statutes include the secure email provider that was required to place a covert backdoor in its product in order to steal users' encryption keys" - and there's a reference here to this in this document, so, I mean, they back all this up with references - "and a consumer electronics company that was forced to remotely enable the microphones in a suspect's automobile dashboard GPS navigation unit in order to covertly record the conversations being held in their car. Outside the United States and other democratic countries, specific statutory authority may be even less important."

Leo: Do they say who these companies are? Or did they just kind of generically, I mean...

Steve: Well, in the references. There's reference no. 18 in the PDF to the second instance and reference no. 2 to the stealing of the email...

Leo: So who was the consumer electronics company? Who was the email company?

Steve: I didn't look. Let me see.

Leo: I guess we can leave that as an exercise for the reader. But, I mean, it does make one wonder.

Steve: Yeah. Well, and I like this because they're raising the point that this has happened. But I have another quote in a second that I'll read.

Leo: Okay, go ahead.

Steve: "The Chinese government, for example, has repeatedly compelled the assistance of telecommunications and technology companies in assisting it with its surveillance efforts. Just as phone companies and email providers can be forced to assist governments in their surveillance efforts, so, too, can SSL Certificate Authorities. The compelled certificate creation attack, which is what these guys have named this, is thus one in which a government agency requires a domestic Certificate Authority to provide it with false SSL certificates for use in surveillance." And I've skipped a bit.

And then they continue, saying, "When compelling the assistance of a CA, a Certificate Authority, the government agency can either require the CA to issue it a specific certificate for each website to be spoofed; or, more likely, the CA can be forced to issue an intermediate CA certificate that can then be reused an infinite number of times by that government agency without the knowledge or further assistance of the Certificate Authority."

So just to finish with one quote, and then I want to talk more about the technology. They have a section called "Evidence," where they describe this device and the device's marketing material. And during this conference, one of the authors of this PDF, this research paper, says, "The company's CEO, Victor Oppleman, confirmed in a conversation with the author at the company's booth the claims made in their marketing materials: 'That government customers have compelled certificate authorities into issuing certificates for use in surveillance operations which are used by their hardware.' While Mr. [Oppleman] would not reveal which governments have purchased the 5-series devices, he did confirm that it has been sold both domestically and to foreign customers."

So the idea that an entity could compel the creation of an intermediate certificate is what is most compelling for me because of what such a capability means when installed into a piece of a hardware. Here's how this works. And what this does is, it allows every single - every single - SSL connection to be eavesdropped on.

Leo: This is the kind of thing that maybe an ISP might do, a company might do, a school might do. Basically a man-in-the-middle attack.

Steve: Well, it wouldn't be a school. It would be, for example, we know, post 9/11 attacks on the United States, that there was extremely broad interpretation of the legal rights of the government to eavesdrop on telecommunications.

Leo: Although I just saw a news story that Gerald Ford approved warrantless wiretaps in the '70s. So...

Steve: Yeah. Well, and remember that a number of telecommunications companies refused to comply.

Leo: But most did.

Steve: But most went along with it. So what we're talking about there, that's an example of the government compelling a company to allow it to eavesdrop on their data flow. So imagine hypothetically that the FBI, by court order, compels a trusted Certificate Authority, any of them, to create an intermediate Certificate Authority certificate. So what that means is that the FBI now owns an intermediate certificate signed by a trusted root Certificate Authority. That intermediate certificate is installed in a device which functions as follows. And say that, for example, this was in an Internet caf. And in fact the brochure for this device says, for example, "This solves the Internet caf problem," as if privacy is a problem in an Internet caf. But, you know, to the spooks it is.

Leo: A problem for them.

Steve: To the three-letter initial people, yes - NSA, CIA, FBI, and so forth. So the way this works is a user somewhere, anywhere, not necessarily in an Internet caf. I don't mean to restrict it. This could be installed in an ISP's facility so that any customer of an ISP working at home initiates a secure connection to anywhere. Anywhere. The packet comes in to this device, to port 443, which is the SSL port. That gives the device the IP that the user is trying to connect to. The device doesn't even have to know what domain this is. And in fact at this point it doesn't know. All it has to do, a SYN packet comes in, trying to initiate an SSL connection. This device sends its own TCP SYN packet to that IP to establish its own connection to wherever the user is connecting to.

What happens then is that the remote server connected to provides its certificate for the SSL connection to the device, to the client that initiated the connection. Now the client, this device, man-in-the-middle device, has the website's certificate. So it now knows exactly what certificate is expected by the originator of this connection. But it knows that, but now it takes advantage of the fact that it is an authentic intermediate CA to build a certificate which it signs on the fly in order to close, to accept the connection originated by the ISP's customer.

So the point is, this is a real-time, practical, man-in-the-middle device which, armed with a trusted intermediate CA certificate, is able to decrypt all SSL connections. And no warnings of any sort ever are displayed on the user's browser. And if they looked at the certificate chain, they would see something they would likely see anyway, which is we often now see, for example, intermediate CAs. And if you followed it back, it would be trusted by somebody you trust. So this is an entirely practical attack, practical right now, presumably going on right now, based on the fact that governments have, we believe, compelled certificates to be issued, and hardware exists for the sole purpose of pursuing this sort of attack. And that's all it has to do.

What I just described is the way this would work. And Microsoft has a PDF document, Leo, which I know you have opened at your end, which is a list of the root certificate program members as of November 24, 2009, so about five months ago, which - and these are the participants in this database that Microsoft maintains. And, you know, there are names. We have the government of Brazil, the government of India, outfit in Spain, Entrust in Canada, Internet Publishing Services in Spain, C-COM Trust Systems in Japan. Another...

Leo: You've got to figure many, at least a few of these are fronts for national security organizations of various countries. I mean, if I'm the NSA, I'm going to set up a certificate root authority.

Steve: Precisely. And you're going to get it installed in the browser.

Leo: Yeah, under a fake name.

Steve: That's a very good point, Leo.

Leo: And it's done, we're done.

Steve: You know, A-Trust in Austria. Bypass, a nice name for one, in Norway.

Leo: And maybe you trust the NSA. But do you trust, you know, the Spanish security authorities, the Czech Republic security authorities? We don't know who these people are.

Steve: Well, and we've been talking...

Leo: Bulgaria?

Steve: We've been talking recently about, yes, exactly, we've been talking recently about China seeming to be behind a number of, well, for example, Google is convinced that China was behind the pervasive attacks against it and a number of other countries. Well, there's a China Internet Network Information Center, CNNIC. They've got a root CA trusted by Windows which is good until 2027.

Leo: Here's one good through 2037 for the Shanghai Electronic Certification Authority, SHECA.

Steve: And we trust, I mean, here's the point, is that all you have to do is get an intermediate certificate signed by one of these organizations. I mean, we're trusting them all. And it means basically everyone listening to this podcast now pretty much needs to assume that at some level these communications are not private. I don't think schools can do this. This is, lord knows, we hope these devices don't get loose and to the point where a school is able to do this. The schools could compel the installation of a certificate in the browsers. So, for example, that's the way the corporate proxies work, where anyone using SSL has to trust the corporate proxy. And that's done by essentially installing the corporate root certificate in the employee's browser. That allows corporations to proxy and monitor SSL connections. But absent that, just using noncorporate, nonemployee browsers, just the browsers we're using now, you need to somehow have the certificates signed by someone you trust.

Unfortunately, it's very clear now that trust has gone completely out of control. I mean, we're trusting everybody on this list. And all any one of them has to do, I mean, this comes back to what I have pounded on our listeners about, which is the bad news about security is, one mistake is all it takes. The entire chain of trust, the entire fabric of security requires perfection. And so one defect is all it takes. And unfortunately we've got 264 possible sources of defects in the fundamental trust anchorage of SSL communications. And thanks to the fact that there is this notion of intermediate Certificate Authorities, once an intermediate Certificate Authority has been signed by a root Certificate Authority whom we trust, then, as I've just demonstrated, it is possible to create a simple device which is able to eavesdrop on all SSL communications virtually without detection.

Leo: That's not good.

Steve: That's not good.

Leo: No. So what do we do? I mean, you need certificates. You need root authorities. I mean, even if it were three, even if it were VeriSign and, you know, I mean, it'd still be this issue of them being subverted. As you just said, the government can order them basically to subvert it.

Steve: Yes. I mean, exactly. Under court order, the law is such that a company can be compelled to provide what the government wants.

Leo: So we - this is something we just kind of come back to every single time, which is, if you want to be safe, don't use a computer. Don't own a computer. Don't get online. That's how you're safe. But is it practical? I don't think.

Steve: No. No. And the reason I bring all this gloomy news up is it's - given this information, I think it's reasonable for our listeners' behavior to perhaps change. Or, if nothing else, for our listeners to be aware that this is very much a possibility, that when they are communicating with their bank, when they are communicating encrypted with Gmail, when they're doing anything over an SSL connection, the fact that they trust the endpoint no longer means that that's the only trust they have to have. Unfortunately, anywhere in that connection there could be a device which decrypts and reencrypts their connection. And in that brief interval where it's decrypted, any kind of packet inspection can be performed, and the decrypter has their IP at the time of connection.

This paper paints a fictitious but typical scenario at the beginning. They say, "A pro-democracy dissident in China connects to a secure web forum hosted on servers outside of the country. Relying on the training she received from foreign human rights groups, she makes certain to look for the SSL encryption lock on her web browser, and only after determining that the connection is secure does she enter her login credentials and then begin to upload materials to be shared with her colleagues. However, unknown to the activist, the Chinese government is able to covertly intercept SSL-encrypted connections. Agents from the state security apparatus soon arrive at her residence, leading to her arrest, detention and ... interrogation. While this scenario is fictitious, the vulnerability is not."

Leo: Wow.

Steve: So I knew that our listeners would want to know. Even if there isn't a great solution for it. I mean, unfortunately, this is the system we have for relying on SSL. It is...

Leo: We're stuck with it. It's not - what are we going to do?

Steve: Yes. It is anchored, it is literally rooted in our trusting of the people that sign the certificates for our web servers and who sign the intermediate certificates. Unfortunately, it's become so popular that everybody wants in on signing. In this document these guys explain that it's reasonable that, for example, some country that uses PKI-signed national ID cards might not want to outsource the signing of their ID cards to some other organization. So they set up their own root CA and convince Microsoft and Apple and Mozilla to trust their root CA. And here of course the problem is the weaker it gets, the weaker it becomes because they're able now to say, well, look at everybody else you trust. Why don't you trust Squamzilla? And it's like, now we've got 264 people that Windows trusts. I mean, literally, anyone you could imagine is on this list.

Leo: Yeah. Well, and in one way I kind of understand that. They might as well just - might as well approve everybody.

Steve: And so that's my point, is it's necessary for us now to proceed with the understanding that at some level it's not - we're not just trusting the other endpoint, which is ideally all we were doing.

Leo: Right.

Steve: Unfortunately, we're needing to assume that this connection is not going to be eavesdropped by the guy who we talked about last week running Ettercap in the coffee shop. We're safe from him, but we're not safe from state-level eavesdropping. We have to assume it exists, and it's pervasive, and it's going on now.

Leo: Steve, as usual, a ray of sunshine. No, it's so important. And I think sometimes people maybe think that, oh, gosh, when I listen to this show I get more depressed. But we've got to know about this stuff. And it just means that you act more intelligently when you're online, that you know what the risks are.

Steve: Right. Well, for example, we already know that security is often leveraged from the point of most vulnerability. So it's certainly the case that you could also get malware in your computer which would be eavesdropping on you before it gets encrypted over SSL. So that's the way Joe Schmoe in the open WiFi coffee shop could get you, is you're sharing a LAN, and you've got a browser hole that is unknown or not yet patched. And so he's able to install something on your computer and eavesdrop on your network connections, even the secure ones, by grabbing the data before it goes over the SSL tunnel. So it's - or somebody could be grabbing it at the other end, after it's been decrypted. And credit cards are escaping on the 'Net all the time, even though they're going over SSL connections. So there's lots of ways these things can leak. This just says, look, here's something that anyone using SSL needs to understand, that at the state level eavesdropping is almost certainly going on. So, as you say, act accordingly.

Leo: Yup. Act accordingly. Steve, it's always a pleasure, always fascinating. You can find more on this at GRC.com. His show notes are there, along with 16KB versions of the show, full transcriptions so you can read along as you listen, and of course all Steve's great stuff, the free stuff like ShieldsUP!, Shoot The Messenger, DCOMbobulator, Unplug n' Pray, Wizmo, Perfect Paper Passwords, and more. And of course the bread-and-butter stuff like SpinRite. In fact, that's the only thing you sell.

Steve: That's the only bread and butter.

Leo: So there you go. That's the only one.

Steve: Everything else is free.

Leo: Although that may change. I know you're working on another product. But for now, go get the world's best hard drive maintenance and recovery utility at GRC.com.