Listener Feedback #121

Description: Steve and Leo discuss the week's major security events and discuss questions and comments from listeners of previous episodes. They tie up loose ends, explore a wide range of topics that are too small to fill their own episode, clarify any confusion from previous installments, and present real world 'application notes' for any of the security technologies and issues we have previously discussed.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-308.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-308-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 308, recorded July 6, 2011: Your questions, Steve's answers, #121.

It's time for Security Now!, the show that covers your security, your privacy online. And who better to do that than the man who's been covering this story since it all began, back with the earliest days of spyware. In fact, he coined the term "spyware," wrote the first antispyware program, and has been helping us with security ever since, Mr. Steve Gibson of GRC.

Steve Gibson: Hey, Leo.

Leo: Hey, Steve. How are you?

Steve: Great. We've got another great episode, #308, and it's a Q&A. It's our 121st Q&A.

Leo: Wow. Your questions and Steve's answers.

Steve: Yeah. Lots of interesting news. A potpourri of goodies. And then some - it's not an overload as we've had the last couple Q&As, so we've got about eight questions, interesting ideas and thoughts from listeners. And we even end it with a Philosophical Question of the Week.

Leo: Ooh, I like that. You know, we just covered the big Facebook announcement right before we went on the air this morning. And one of the things I noted, at least on the Macintosh, I haven't checked it on Windows yet, is that it does install itself using Java, the Java archive. So one of the things I'd like to ask you about in a second is how you feel about that, given the security exploits that it's been riddled with in the last...

Steve: Well, that's a problem. And then the other problem is that it is actually Skype in a box. And so what Facebook is using is essentially repackaged Skype technology. And as we know, Microsoft bought Skype recently for $8.5 billion. And what popped up on the radar this week is the fact that Microsoft just acquired a patent which they filed for a couple years ago about how to surreptitiously eavesdrop on a peer-to-peer VoIP system.

Leo: We will talk about that in great detail. Oh, boy. All right, Steve. Let's get to - I guess we always like to start with security updates.

Steve: Yes, and we've had a very quiet week this week, not much going on. Of course next Tuesday will be the second Tuesday of the month since we had, well, the Fourth of July of course was last Monday, so the 5th is Tuesday. So I expect we'll have some news, yes, we'll have some news next Tuesday, but nothing this Tuesday.

An interesting note was picked up by someone who noted that a security company, SecurEnvoy, was applauding the LulzSec folks.

Leo: Really.

Steve: Which I thought was sort of interesting, yeah. Net-Security.org had a blog posting that said, "In an unexpected move for a security company, SecurEnvoy today said that cyber break-ins and advanced malware incidents such as the recent DDoS attack by LulzSec should actually be welcomed and their initiators applauded. Explaining this sentiment, Andy Kemshall, CTO and co-founder of SecurEnvoy, said, 'I firmly believe that the media attention LulzSec's DDoS attacks [and other break-ins have] recently received is deserving. It's thanks to these guys who are exposing the blas attitudes of government and business without any personal financial gain that will make a difference in the long term to the security being put in place to protect our own personal data.'"

Leo: That's effectively what LulzSec and these other grey hat hackers use as an excuse, people like Adrian Lamo, for what they do.

Steve: Right.

Leo: They say it strengthens security. We're on the side of good, not evil.

Steve: And so they're right. I mean, I'm not - we can't condone the breaking of the laws which unfortunately are the means by which security gets strengthened. But it really is

only a consequence of these sorts of breaches that companies take action. It must be as a consequence of this recent flurry that really came to high profile, I mean, I was seeing conversations about these Internet web break-ins on non-tech channels of information that wouldn't normally be covering it because it really did come to the attention of the press, and certainly to the attention of other companies who, as I've said many times, their CEOs must be asking their CIOs, tell me this isn't possible, tell me our passwords are encrypted, tell me all of our data is encrypted. And it's very often the case that the Chief Information Officer would say, well, no, that's on our list of things that we'd like to get to, but you keep us too busy dotting our I's.

Leo: This is why you applauded Firesheep.

Steve: Yes, yes. And we did see an absolute reaction to Firesheep. It got cited, and it was downloaded a million-plus times. And now companies like Facebook are enforcing persistent HTTPS, clearly as a consequence, I mean, absolutely. It was not any coincidence that that got added after Firesheep did. So, and here's Sony that's become a laughingstock in terms of the number of attacks. And as we'll see a little bit later on in this podcast, they got another one yesterday.

So, I mean, it's unfortunate that the only thing that moves companies to make themselves more secure is this kind of high-profile breach and attack and embarrassment. And we know that there are going to be lawsuits that will follow these things that won't be on our radar as much as the technology that portends the future suit. But that's happening, too. So I don't know that I would say I think it's great. But it is the way the world works.

The reason Microsoft has gotten as good as they have about security is not because they wanted to, it's because they had no choice, because Windows had become a laughingstock. It was a catastrophe from a security standpoint. And Microsoft, though it took a long time and was very slow, they finally did step up. They would not have. And we would have a much less secure OS today were it not for the fact that there were hackers poking at Windows for so long and so successfully that Microsoft begrudgingly got around to it.

Again, all of this feels to me like frontier land. I mean, we're just - in a decade from now we're going to have to come up with a new name for the podcast, Leo, and - well, maybe 15 years - and switch topics, Technology Today or something. Because these problems are going to get themselves solved. But right now we've got a real place.

Leo: Yup. I'm glad you're going to cover this Dropbox thing because I didn't - I saw it, and I didn't know what to make of it. So I'm curious what you say because I use Dropbox like crazy.

Steve: I know you do. And in fact I got email from them because you and I were using it to transfer podcast audio for a while.

Leo: That's right, yeah.

Steve: Yeah. So in the wake of the problems, the security problems that they had -

remember that we've talked about several things: the revelation that they were able to decrypt the data, which they had not made clear before; and then they had the four-day - or four hours, rather, excuse me, four hours during which time their passwords were not required to log into a Dropbox account, so anybody could log in who wanted to. They did a revamp of their Terms of Service, and several things caught my eye.

First of all, the letter that I received, the email that I received, as all Dropbox users would have, said, "Hi, Steve. We wanted to let you know that we've made some changes to our Dropbox Terms of Service, Privacy Policy, and Security Overview. We did this to make our policies easier to read and understand" - and I have to agree, they are - "and better reflect product improvements we've made to Dropbox. Please read about these changes in our blog post and read the docs themselves." So I...

Leo: I didn't read them. I just thought I'd let you read them and tell me about it.

Steve: That's what I'm here for. And I pulled interesting bits out of the otherwise legalese boilerplate, although they've really made it much more clear. So under Security Overview they said, "Like most online services, we have a small number of employees who must be able to access user data for the reasons stated in our privacy policy" - which I'll discuss separately in a second. And then they say, "e.g., when legally required to do so." So that's a clear acknowledgment that, if they were served with a court order requiring that a given user's data be turned over to some three-letter initial organization that works for the government, they would do so. Then they say, "As set forth in our privacy policy" - well, okay. I should say they would and can do so. So they're making that clear.

"As set forth in our privacy policy, and in compliance with United States law, Dropbox cooperates with United States law enforcement when it receives valid legal process, which may require Dropbox to provide the contents of your private Dropbox. In these cases, Dropbox will remove Dropbox's encryption from the files before providing them to law enforcement." So very clear there for those people who...

Leo: Not everybody has to do that, by the way. I mean, that's something they've decided they want to do. I think that should be made clear.

Steve: Wait, they've decided that they...

Leo: They want to be able to provide the data to law enforcement. They could have a system, there are many companies that do, where it's pre-ingress encryption, as we've talked about, pre-Internet encryption. And they just say, yeah, we'd give you that information, but we don't have the keys.

Steve: Well, and case in point is LastPass.

Leo: Yeah. Or what I use instead of Dropbox for my private stuff, Wuala, which encrypts before it goes to the Internet. They don't have the key. So they could - there's no legal requirement that they have to be - or is there?

Steve: Ah. There actually is a reason they do this, and we'll be talking about that in a second.

Leo: Oh, good.

Steve: It's really interesting, too. And it's been hacked. So...

Leo: Oh, even better.

Steve: So they also say, "Dropbox applies encryption to your files after they have been uploaded."

Leo: Post-Internet encryption.

Steve: And separately I should say that they do encrypt in transit. So they use standard SSL 256-bit encryption in transit. But when they receive it, it's back out of SSL in plaintext. Then they encrypt it for storage. But not until they do something else, but I'll get to that in a second.

"Dropbox applies encryption to your files after they've been uploaded, and we manage the encryption keys." "We manage," they say, "the encryption keys. Users who wish to manage their own encryption keys can apply encryption before placing files in their Dropbox. Please note that if you encrypt files before uploading them, some features" - which we'll be discussing in a second - "will not be available, such as creating public links. Doing so will also make it impossible for us to recover your data if you lose your encryption key." And of course that's the whole point. So that was their Security Overview, the highlights of that. Under their Privacy Policy, they said, regarding files: "We collect and store the files you upload, download, or access with the Dropbox service.... If you add a file to your Dropbox" - get this, Leo - "that has been previously uploaded by you or another user, we may associate all or a portion of the previous file with your account rather than storing a duplicate." So they're doing...

Leo: To save space.

Steve: ...duplicate elimination, yes. Okay. Under Data Retention - and we'll come back to that in a second. Under Data Retention they said: "We will retain your information for as long as your account is active or as needed to provide you services. If you wish to cancel your account or request that we no longer use your information to provide you services, you may delete your account." But, "We may retain and use your information as necessary to comply with our legal obligations..."

Leo: So in other words, you could kill your account, delete your information, and they would have a copy which they would retain.

Steve: At their discretion, yes.

Leo: Is this related to the FBI demanding that ISPs retain two years' worth of data?

Steve: Could very well be. They said to "...resolve disputes and enforce our agreements," which they don't specify. "Consistent with these requirements, we will try to delete your information quickly upon request. Please note, however, that there might be latency in deleting information from our servers, and backed-up versions might exist after deletion. In addition" - so they could have, you know, squirreled-away copies that continue to exist persistently. "In addition, we do not delete from our servers files that you have in common with other users." And then finally under Security of their Privacy Policy, they said, "We follow generally accepted standards to protect the information submitted to us, both during transmission and once we receive it. No method of electronic transmission or storage is 100 percent secure" - certainly not ours - "however. Therefore, we cannot guarantee its absolute security." So they've given themselves a final out there.

Now, this got me really curious about what this dup elimination system was. And I remember years ago talking to a company who was - they were just at the startup Internet backup kind of concept stage. And one of their clever ideas was to note that many of the files that users using a common OS would have on their system would be duplicates. All these DLLs, well, they all came originally from Microsoft or from applications that we loaded. And for those that are of the same version, they're identical. So they were early on...

Leo: Who's backing up their operating system or binary application folders? I mean, isn't it data that we use this for?

Steve: Well, largely. But their notion was, due to the extremely high level of duplication, that is, yes, the binary folders are huge, but they're also full of stuff that absolutely will be identical...

Leo: Of course.

Steve: ...across a huge population of users. Which means you don't actually back them up. You back up a couple of them, and then when you see that the same user has the same file on their system, all you do is store a pointer to the master copy. And so you save all of this actual shuttling back and forth and storage. You simply do a hash. Well, that's what Dropbox does.

Leo: You know, by the way, I'm going to point out the real point of this is that - music and movies.

Steve: Yes.

Leo: And these are large files; and, sure, they save space. But even more to the point, they also - I think this is a response to the recording industry and the Motion

Picture Association of America. And, I don't know, it just makes me nervous. I'm going to use more Wuala and less Dropbox.

Steve: Yeah. So, okay. So someone figured out what the Dropbox client API was. They reverse engineered it. And if you look under "Dropship" under Wikipedia, you'll find a tool which was created by someone who reverse engineered this. What they realized was, this was better than BitTorrent. So what happens is, the way Dropbox works is in 4MB blocks, an SHA-256 hash is made of the block. And that is sent to Dropbox to see if they already have it. And if they already have it, then the file is not transferred to Dropbox. Merely your account is tagged as having this file, too, and it instantly appears in all instances of your synchronized Dropbox folders.

So what this does is it hugely, exactly as I was saying before, reduces the storage that Dropbox needs to maintain because any duplicate AVIs, any duplicate MP3s, any duplicate anything gets hashed and checked to see if it's already there. Which means from a mass distribution standpoint someone loads one copy into their Dropbox folder, and then distributes the hash. And so Dropship consists of two files, or two EXEs. The dropship itself is a tool for injecting a file into your account using its reverse-engineered-from-Dropbox description. And then the second tool is called hash_blocks, which produces a description from a file that can be used by dropship. So everybody gets a copy of Dropship. And I want to send somebody a file, or a huge audience, or post it somewhere on the 'Net. People - we produce, using hash_blocks, produce a description which is the hash of these 4MB blocks; send that, which is super small, to broadcast it or send it to a large audience. They all simply take that and put that into Dropship using the dropship tool which injects that into their account, and suddenly that big file appears in everyone's Dropbox folder. So very clever.

Leo: Although, I mean, you have the public folder capability. And since - I guess this is better than you putting it there because...

Steve: Yeah, it was just sort of done as a hack. I mean, it was...

Leo: It's a cool hack. By the way, Dropbox says they've disabled it.

Steve: Yes. And it wasn't done painlessly. This all occurred in March, a few months ago. And Dropbox immediately tried to shut them down, asked that they remove it, generated some bogus DMCA takedown notices, although, you know, claiming that this code was a violation of the DMCA although it was open source, it was reverse engineered from their protocol. So essentially what they had was a weak technology for doing this.

The problem is, as we know, no matter what they do on the client side, if they're going to continue to try to do this, and I'm sure they are, all they would have done would have been to add some further layers of obfuscation. Any client, as we've often said, the protocol can be reverse engineered. So there's nothing to prevent someone from creating some software that does mimic the normal operation of Dropbox, that is, normally the only way a user could generate the hash on their system would be to actually have the file and physically hash it and then have the Dropbox client check to see if they already have a copy, which would save Dropbox the bandwidth and the user the time of uploading it. Which is cool. But so what this approach does is this short-circuits the

process so that you don't actually ever have to have the file in order to have it appear in your own Dropbox. And so essentially that's what this does.

Leo: Chetpod (sp) in the chatroom asks an interesting question. Is it possible that there are hash collisions, that you could think you had a duplicate of a file, and it was just a duplicate of the hash?

Steve: Yeah. Wouldn't that be disturbing.

Leo: That wouldn't be good.

Steve: Yeah, not good.

Leo: Especially if it's a DLL or something.

Steve: Yeah. With an SHA-256 we've got, I mean, that's a huge number of bits. And it has to be an exact match. The hash is very mature and well designed. So it's incredibly unlikely that there would be a collision. I don't know that they're also storing the size. I would bet, if they're doing it right, they're storing the size also because that's a tiny bit of additional information. And to have the same size and a hash collision, that's just not going to happen.

So but it's a great question because that's absolutely the case that a hash collision would confuse the system, and you would download - you would upload your file and go, wow, that was quick. And then when you tried to download it, it would be a different file because the system would have thought you were uploading one it already had, and when you downloaded it, you'd get the wrong one in the instance of this collision. But SHA-256 is so secure. I mean, we're relying on it for many other things much more important than disambiguating Dropbox blocks. So I think it's, I mean, it's a good theoretical issue, but in practice not a problem. But we do have a problem.

Microsoft has obtained a patent for specifically intercepting Skype conversations. This is their application 20110153809 called "Legal Intercept." And in the abstract at the top of it, it said - I'm reading now from this: "Aspects of the subject matter described herein relate to silently recording communications. In aspects, data associated with a request to establish a communication is modified to cause the communication to be established via a path that includes a recording agent. Modification may include, for example, adding, changing, and/or deleting data within the data. The data as modified is then passed to a protocol entity" - this is all patent speak - "that uses the data to establish a communication session. Because of the way in which the data has been modified, the protocol entity selects a path that includes the recording agent. The recording agent is then able to silently record the communication."

And skipping down then to paragraph 28 of the details, it says, "As mentioned previously, traditional techniques for silently recording telephone communication may not work correctly with VoIP and other network-based communication technology. As used hereafter, the term VoIP is used to refer to standard VoIP as well as any other form of packet-based communication that may be used to transmit audio over a wireless and/or wired network. For example, VoIP may include audio messages transmitted via gaming

systems, instant messaging protocols that transmit audio, Skype and Skype-like applications, meeting software, video conferencing software, and the like."

And then separately cited in an article about this, Jeffrey Chester, who's the executive director for the Center of Digital Democracy, said the technology aligns with Microsoft's broader goals. The company "aims to incorporate tracking technologies for its Skype services as it aggressively expands its mobile advertising system across the world. Skype will likely soon have ad targeting and user-profiling digit strings attached. This underscores the need for strong mobile and location privacy safeguards."

So we've talked a number of times because there has been this grumbling in the U.S. Congress about their response to our law enforcement's concern, which is certainly understandable, that they are no longer able to eavesdrop on an increasing percentage of Internet traffic. And so, as we know, there has been talk of legislation that would require services to allow the service provider to respond to a law enforcement request for eavesdropping and decryption. And specifically Skype had been immune to this because as you and I know, Leo, we have a point-to-point communication. That is, Skype's encrypted, and encryption technology is extremely good. And but moreover, our data is going between my endpoint and your endpoint over an undecryptable connection.

Well, Microsoft bought Skype and is now clearly in the process of adding this technology, which will break the encryption, allowing essentially technology for a by-design man-in-the-middle attack which will cause our endpoints to, at their discretion, to no longer establish a point-to-point connection, but to deliberately route the data through a, as they said, "silent recording entity" which would decrypt it and then make it available.

Leo: I should point out that it's possible that Microsoft's patenting this to keep somebody else from doing it. Sometimes you patent things defensively. So it may mean merely that they know this technique exists, they know it's out there, and they want to patent it to keep somebody else, I mean somebody legally from doing it. Of course by publishing it they're making illegal usage even easier, if you don't care about patent infringement.

Steve: Yeah. And there really isn't a practical way for someone, for example, to do this to a Skype conversation. I mean, the way you get around, the way you solve this encrypted link problem is that you get an agent running pre-encryption at either end of the conversation. So there is still that.

Leo: So you have to build it in. It's not something that exists now. You'd have to build it into Skype.

Steve: Yes. It's very clear that it doesn't exist now, and that Microsoft will be giving us newer and better versions of Skype in the future, Leo.

Leo: Is this, do you think, a response to that legislation that kind of requires this...

Steve: I think that's exactly what this is. I think if Microsoft decided we're going to buy Skype for $8.5 billion, and if legislation does get passed and Microsoft...

Leo: It hasn't been passed yet.

Steve: Right. It hasn't been written yet. I mean, there's been a serious back pressure against law enforcement wanting this. And so, I mean, it really raises concerns about abuse that we do see happening when law enforcement gets technology that they don't know how to handle correctly. So it makes total sense to me. Microsoft's going to spend $8.5 billion on this technology, they're not going to risk having legislation passed that would outlaw that technology. Which is exactly my concern that I've discussed with my doing a VPN because, in the same way that Microsoft might be compelled to put a backdoor in, so could everybody else who's trying to sell something commercial that is really robustly secure, as Skype up till now has been. So...

Leo: Oh, well.

Steve: ...this is Microsoft saying, well, we're going to offer Skype, but we're going to do it so that we can eavesdrop if we have to. Okay. Now here is - this is sanity check time, Leo. The URL is IsMyCreditCardStolen.com.

Leo: And let me ask. Do you enter your credit card number?

Steve: Oh, just look at this. Look at this website. And this is basically an IQ test. This is a test that many people who don't listen to Security Now! might fail. I hope that no listener of this podcast would fail this test. IsMyCreditCardStolen.com.

Leo: But, see, it says "Verified Secure" right on the front page.

Steve: Isn't that comforting? Yes. So we've seen...

Leo: [Laughing hysterically] I'm sorry.

Steve: I know. We've seen, you know, has my password been hacked, has my email been stolen, has Sony been hacked, I mean, this is the new vogue style of website. So now we have IsMyCreditCardStolen.com. And it asks you, put in your credit card number, put in your name, put in your expiration, I mean, I'm looking and thinking there's no way I'm putting this stuff in. So, Leo, go ahead and click the button without putting anything in.

Leo: All right, let me see. So check right now, okay.

Steve: Just don't put anything in.

Leo: "Don't worry, your credit card details weren't transmitted when you hit the Submit button, but don't trust this claim without question. Find a technically inclined friend to verify it for you. After all, you've already been tricked once." Oh, good, so it's a good guy.

Steve: It is a good guy. Before I clicked the button I got the page source, and I read the source code for the page. And it's actually been very well designed.

Leo: This is great.

Steve: Isn't that great?

Leo: Oh, good for them. Oh, that scared me for a moment.

Steve: Oh, it ought to scare everyone. And, I mean, it's like, oh, yeah, let's just see if this information is part of some public database. It's like, oh, my goodness. And it's not SSL. It's not secure. I mean, there's nothing about this that says, oh, yes, please put your credit card information in here. So I just love that, IsMyCreditCardStolen.com.

Leo: Brilliant.

Steve: Yeah.

Leo: I'm going to put this out on my Twitter and see how many people go to it.

Steve: Oh, goodness. Be great if they were collecting statistics. They aren't. They're doing nothing evil with it.

Leo: Fortunately.

Steve: And all the Submit does is...

Leo: Oh, this is from the Anti-Phishing Working Group. These people are great, actually. I know them very well. It's a great website that has - they keep actually a wonderful database of phishing emails on here. So this is, yeah, they're good, they're good. Wow, this is great. How funny.

Steve: IsMyCreditCardStolen.com. Oh. Any idiot...

Leo: What they should do, put up a big sign: "It is now."

Steve: Oh, gosh. So under Attacks & Breaches we do have, as I mentioned earlier, Sony got hacked yet again. This was the Sony Music Ireland website that was hacked. And three very distressing to music lovers news stories, bogus news stories were posted on their home page. And I don't follow current musicians and bands in Ireland closely enough to be disturbed by these or even to have remembered. But they went to great extremes to say, oh, no, no, these people are not dead. These groups are not disbanded. So I guess it caused some uproar, as it was clearly designed to. So HasSonyBeenHackedThisWeek.com? Yes, once again, it was just on 7/5, on July 5th.

Leo: How many is this now?

Steve: Oh, goodness.

Leo: 25?

Steve: There's a summary. Is it 25 or 27? I don't remember. Has Sony been hacked...

Leo: I'm entering it in. It was 20 the last time I checked, so...

Steve: Yeah, HasSonyBeenHackedThisWeek.com.

Leo: Has Sony been hacked dotcom.

Steve: This week dotcom.

Leo: This week dotcom, all right. And the answer is, not surprising, yes. And let's just see here how many hacks there have been. Latest hack was July 5th. Sony's hack history going - you know what? They don't even count. They've lost count.

Steve: I thought there was a count on that first page.

Leo: There was, and I think they stopped. But this looks like the 21st hack. There was. They no longer have a count. It's like...

Steve: Sony was joined by a rather high-profile company that was embarrassingly hacked: Apple.

Leo: Yeah.

Steve: Apple's business intelligence site was hacked by the group that calls themselves Anonymous. And in order to prove that they had hacked that Apple site, they tweeted a link to a Pastebin page where usernames and passwords which had been taken from an SQL database there were posted. Apparently there was a SQL weakness of some sort. And so Apple's business intelligence site, which was then taken down immediately in order to figure out what was going on and solve the problem, got hacked. And speaking of this, we should follow up a little bit on your real-time news from last week, Leo.

Leo: Yes, because we were hacked. And let me just see what the latest story is on this because we did get some updates from our sysops.

Steve: Because I remember someone changed a few lines in jQuery, the jQuery library, the very popular JavaScript query library.

Leo: We have three servers that provide live.twit.tv. And one of the three jQueries was modified. It's my understanding that it was through an old install of WordPress that was sitting on one of the servers and hadn't been updated in some time. WordPress is really notorious for having lots of flaws in it. We have of course removed that instance completely because it was an old blog we haven't kept up. It was for a show we did years ago.

Steve: Actually, this is a really great tutorial in the way somebody bad gets into a system is some software that you were using, that you switched away from, but it stayed there and accessible online.

Leo: The good news is that we had other checks in place that kept the hack from installing - it was intended to install a rootkit on visitors to our site. But the other checks we had in place kept it from doing that. So it was a modification in the jQuery library. People who saw that popup from Chrome and other spots, other places, antivirus software and so forth...

Steve: Which is very cool.

Leo: ...saw that line. But what did not happen, I'm told, and Bear is really good, is that no malware was in fact put on anybody's system because of other security software.

Steve: Safeguards that you guys have, yeah. Good.

Leo: So really what happened is that a file essentially got corrupted, with no other damage done.

Steve: So following up on last week's podcast about identity, a friend sent me a link to a Google initiative where Google has produced a kit which they would encourage other websites to use - it's free - which would allow visitors to log into those websites using their logins from other sites. This is the OAuth technology that we did a podcast on. It was Episode 266, Security Now! Episode 266, if anyone's curious. And I did refer to that also last week.

But then I found something even more extensive. It's called Hybrid Auth. It's at SourceForge, so hybridauth.sourceforge.net. And this is, again, another open source project. It's a PHP package which is exactly this, but even more comprehensive. Using this, any site which already had PGP support at their server side, could allow users to, first of all, create an account on that site if they wanted to, or use any of their existing accounts at Twitter, MySpace, all of the Google assets - so Gmail, Orkut, YouTube, et cetera - Facebook, Tumblr, Friendster, OpenID, Foursquare, LinkedIn, Yahoo!, Gowalla, Vimeo, Windows Live, and PayPal. So, I mean, this occurs to me as a really - this is a great direction for sites to be going in. I'm glad Google is doing this, and I'm really glad that this Hybrid Auth project exists.

So just to be clear, what this means is, how many times have we, surfing around the 'Net, gone somewhere, and in order to do anything, we have to create an account, which is really annoying. If it's just to post a comment on a blog, I mean, I'm sure there are many few comments on blogs for sites that require you to create an account before you can do that. And in fact statistics are now being taken of the relative rate of account creation, or for example doing the things that you would be able to do if you create an account versus losing people who don't; or giving them this choice, to authenticate themselves through a different site and then get credentials back from that site.

And the statistics show, I mean, exactly what you'd expect. Users are delighted to use their existing Google authentication or their Facebook authentication in order to identify themselves securely to some random obscure third-party site that wants to know who they are, but currently the existing model is requiring that you go through all of the nightmare and annoyance of creating an account. Just not necessary. So at hybridauth.sourceforge.net is a link to the home of this project, Hauth.sx33.net. So I went there because I wanted to experiment with this. And it has, like, a sample how this would look. And there's, like, create your account on the left, or logon to this site using any of those logons on the other sites.

So I clicked Google, and I was redirected to a secure HTTPS Google.com sign-in page, which I see all the time, and I verified the credentials, and everything looked right. I got a big green EV certificate verification. And in fact LastPass quickly filled in my information for me, so all I had to do was kind of like make sure this was what I wanted to do. And on the page it said "Hauth.sx33.net is asking for some information from your Google account. To see and approve the request, sign in." So I signed in. And then I got to - it took me to accounts.google.com. And actually my favorite Certificate Patrol add-on for Firefox popped up because I had never used - because Google has a *.google.com certificate where they've got, like, sites and docs and accounts and anything dot google.com. So they have one certificate that handles all that. But Certificate Patrol notifies me of any different instance of its use that it hasn't seen before.

So I had not yet had an occasion to go to accounts.google.com. This brought me there, where I was still - so I was at Google, and it showed me Hauth.sx33.net is asking for some information from your Google account. And then it showed me the account name, my account name at Google. And then it enumerated what information was being requested - my email address with my name and my email account; my language, English; and my Google contacts. And then I had the choice of saying Allow or No

Thanks, and also to remember this approval for the future. And when I said Allow, I was then redirected back to that original site that just for the sake of this demo showed me a breakdown in detail of exactly what it was they had received from Google.

So this is tremendous. This is what we need to have happen for all of those sites that want some authentication of their users, but that are currently losing people because of the annoyance of having to create an account. This solves the problem using OAuth, whose initial security problems that we discussed in Episode 266 have since been fixed by OAuth WRAP, which is sort of the follow-on successor to it. And I just hope we see this more and more. If my site had any purpose for creating accounts and logging people in, I would do this in a heartbeat because, I mean, just for no other reason than to encourage it. This is a slick, simple way of beginning to add really useful cross-site authentication, and it's robust from a secure standpoint.

Leo: Bravo to standards.

Steve: And I got from Certificate Patrol, speaking of them, my most scary warning yet, and it was wonderful. And it was when I went to GitHub. I don't remember what took me to GitHub, but something preparing for the podcast today did. And so Certificate Patrol popped up, and it said, "Certificate exchanged, reason to worry!" (exclamation point) at GitHub.com. So and then in the details it said, "Warning: This certificate wasn't due yet." But it's like, okay, well, we've had that before. It said, "Maybe there are other reasons why it needed to be exchanged, though." Then it said, "Alert: Host name has changed. Take a look if that's okay." And then it said, "Caution." And here's the big one. "Certificate authority has changed." I just - I love this add-on.

So then it shows me the old certificate, which was *.github.com. The new certificate was issued for just github.com. So for whatever reason they just decided not to do a wildcard certificate. They just did a regular certificate. So that was the name being changing part. But then I looked down, and it's like, oh. The old certificate was issued from GoDaddy Secure Certificate Authority. The new certificate was issued by my new favorite, DigiCert.

Leo: Yeah.

Steve: And that's where I'm going, too, because they provide all the same services. We'll remember that that's what Facebook is using. And it's DigiCert High Assurance EV CA-1. So GitHub said, we're not paying for a GoDaddy EV certificate because they're so expensive.

Leo: What, they're thousands of dollars; right?

Steve: Yes. We're going to go to DigiCert and get their High Assurance EV, and I'm going to do that, too.

Leo: How much is their High Assurance EV?

Steve: I don't remember, but it looked like something that I was willing to do.

Leo: Not 2,000 bucks.

Steve: Where it's just, like, not going to happen over with VeriSign or any of these other big guys. And all we need is it to be a legitimate, good Certificate Authority that is present in everyone's browser. And if Facebook is using them, then they're present in everybody's browser.

Leo: Right.

Steve: So I just love this Certificate Patrol. It is very cool. I want to just bring it up again to recommend it to the one user of our podcast who hasn't yet installed this, to recommend that he or she do so because it's cool information that you just get easily.

Also in Miscellany I ran across - I just wanted to mention for those interested in bitcoins, BitcoinCharts.com is amazing. It is tracking all of the various Bitcoin exchanges, showing exchange rates and volumes and charts and so forth. So anyone who's been playing with Bitcoin, I know we have a lot of listeners who do because I see a lot of tweet feedback about Bitcoin stuff: BitcoinCharts.com.

Leo: So what's interesting, and I'm not surprised, is that some of these guys are not giving you full value for your bitcoin.

Steve: Uh-huh.

Leo: So they've marked those in red, and then green are the ones that are giving you good value. And then there are some that are just kind of like, what? What? $42? What?

Steve: Yeah, it's like, I don't know.

Leo: Here's one that's bidding $651 and asking $890. That's got to be - that's all messed up. But anyway, this is good. This is great.

Steve: That's a low traffic exchange, or zero traffic exchange.

Leo: Zero traffic. But everybody uses MtGox. I mean, that's kind of the definitive one.

Steve: Yup, that's the one. Okay, now, I've got something that just rocked my world in the last week that old-timers like you and me, Leo, will certainly understand.

Leo: Yes, we will.

Steve: And this is the news that, for the first time ever in North America, in the United States, our power line frequency is going to be allowed to drift away from 60 Hz.

Leo: Yeah, I don't know if it's the first time ever. I think - by the way, we covered this on the radio show.

Steve: Okay.

Leo: Somebody called in, and I said, huh? And then I heard from some power line engineers who said that in the early days it was routine that it would drift. And then we put in a lot of very expensive equipment not so long ago, a few decades ago, to make sure it was locked into 60 Hz.

Steve: Well, and what used to happen that I really loved was you could actually see, if you had a really accurate reference, you could see during hot summer days that your clocks that were driven by the power line would fall a little bit behind because the speed of the generators in the dams would slow down, or in the nuclear power plants would slow down because of the load that they were pushing. But then at night or on cooler days they were literally tracking how many cycles they were behind. And so they would then run the generators faster in order to make up for that slump time so that your net frequency over a large period of time was still locked at exactly 60 Hz. But what's apparently going to happen now is they actually are going to allow it to drift off.

Leo: It's expensive to keep it locked.

Steve: Yes. So the blurb that I found, the best one I found said: "The North American Electric Reliability Corp. runs the nation's interlocking web of transmission lines and power plants. A June 14 company presentation spelled out the potential effects of the change: East Coast clocks may run as much as 20 minutes fast" - fast - "over a year, but West Coast clocks are only likely to be off by eight minutes. In Texas, it's only an expected speedup of two minutes."

Leo: So in the worst case it's not a whole - it's a few seconds a day.

Steve: Yes.

Leo: It's not a huge drift. It's not all of a sudden you're going to be late for work.

Steve: Correct. And this is also only clocks that actually get their time reference from the power line. Now, your typical cheesy $7 LED clock that you plug it in and then it blinks 12 until you set it, those are probably, they may not have a crystal reference because it's so

easy to simply count the cycles of AC coming in. That's incredibly inexpensive. So very inexpensive clocks do this. It may very well be, though, that better clocks are not trusting the AC line. Certainly a clock that runs at either 50 or 60 Hz, it would have its own internal time reference, not using the AC line. So anyway, that just...

Leo: And it's not expensive to put a crystal in there.

Steve: Not any longer, true, true.

Leo: And NIST was at great pains to point out that their cesium clock will not be affected by this. The atomic clock is still precise.

Steve: Wait, it's not plugged into the wall, Leo?

Leo: No. Wouldn't it be funny if it were?

Steve: Oh. What happened to the cesium clock? Oh, someone tripped over the cord. I just hate when that happens.

Leo: So this actually, this started in 1930 that they kind of tried to keep this up. So it's interesting that this is a big change. And people asked about my computer, or your computer. Your computer is not going to be affected by this. They all use crystals.

Steve: No, yeah, our computers definitely use an on-motherboard time reference. And now that we're tied to the Internet, we're also pinging one of the Internet time servers and being synchronized all the time. In fact, I just downloaded a really cool app for the Pad, and I think it's available for the iPhone. I just searched in iTunes for "atomic clock," and I found one where the description made it extremely clear that this was exactly what I wanted. And that is, when you start it, it shows you that it is synchronizing, and it sends out pings to time servers, and you can configure it for which time server to use in order to lock itself down to - they used some strange word I hadn't seen, it's like femtoseconds or something, but it wasn't that. It's like...

Leo: It's a very small second.

Steve: ...okay, folks, I'm sorry, but you're not that accurate over the Internet because we've got packets.

Leo: Well, it may be NNTP would be a good topic someday for a Security Now!. But I've always thought you're not going to be that accurate. You could still be a second or two off due to latency from the Internet; right?

Steve: You always will be, yes. Well, not a second or two. But down in the low milliseconds.

Leo: Depending. I mean, it depends on your Internet connection. And so we have this kind of notion that, oh, this is exactly right. In fact, it might not be. It might be half a second off.

Steve: Well, there are clever things you can do, though, Leo, because for example, if we assume that packet transit time is symmetrical, when you send your query off, you see how long it takes to get the response. And so you're able to assume that, if we have symmetrical transit times, that the actual response was sent half of the time that it took the roundtrip. So you're able to null...

Leo: Right. You can get pretty close, in other words.

Steve: Yes. You're able to null the delay out that way. But people with satellite links, sorry, folks.

Leo: I would very much like to do a little bit on NNTP. And somebody in the chatroom has given us a wonderful link, Time.is, which is a web-based atomic clock. But I don't believe, unless I'm misunderstanding it, it's getting the time, as most web-based clocks do, from the JavaScript from my system, but in fact it's getting the time - it's giving me server-side time accurately updated, I would hope.

Steve: Yeah, we hope.

Leo: Otherwise, what's the point?

Steve: Okay. Now, my last bit of Miscellany I tweeted because when my buddy told me about this I thought it was one of just the cleverest and coolest things I'd heard of in a long time. His smoke alarm died, and he's got really high vaulted ceilings, and he actually wanted me to come over to spot him while he was, like, at the top of a scaffolding ladder, leaning out, trying to get to it. And I said, well, I'm right in the middle of coding right now, Mark.

Leo: Get somebody else to hold your...

Steve: I'll see you in a couple of days.

Leo: If you die, I'll smell it, and I'll let you know.

Steve: It was beeping at 4:00 a.m. It's like, okay, I know that's annoying.

Leo: Oh, I do hate that. We did a whole TWiT with Kevin Rose. He was at his parents' house, and the smoke alarm beeped the whole show.

Steve: Okay. Get this. They are now available, I know that Lowe's carries them, I think First Alert is the brand. You can silence and test the smoke alarm with any IR remote control.

Leo: What?

Steve: Isn't that the coolest, cleverest thing, Leo?

Leo: I need that.

Steve: It is so cool.

Leo: Wait a minute. So, okay, every time I cook bacon my alarm goes off. Whoever put a smoke alarm, like, three feet from the stove, not thinking. So you're saying I can aim an infrared remote at it, and it would turn it off?

Steve: Yes. Isn't that fantastic? We all have one, and it uses an IR remote.

Leo: I go, and I'm waving something at the thing like this.

Steve: The remotes generate a modulated IR, so it's not going to confuse that with, like, the heat from a real flame. That won't confuse it. So it sees a fast modulated IR coming in, and it takes that as a command. And so you do it three times in order to test the battery, and it goes doot doot doot doot, and it's like, okay, cool. So you don't have to climb up and push the button or throw a tennis ball at it or something.

Leo: Wait a minute. Is this a feature built into smoke alarms?

Steve: New smoke alarms.

Leo: Oh, no, so my old ones may not work. But the new ones all do this.

Steve: Oh, no, no, no. Absolutely not. This is - I had never heard of this before. So this is a...

Leo: So they have built in an IR receptor that you can go blink, blink, blink, and it's

great, you don't have to press the button to test it.

Steve: You don't have to climb up and so forth. And if it goes off - mostly, as you said, smoky bacon, and it's, like, annoying - you just, you don't have to get, you know, get on your ladder or your stepping stool, you just use any IR remote, which I just think that's the clever award of the year.

Leo: I'm going to buy these. I've got to find them.

Steve: I just - I love it.

Leo: Yeah, brilliant.

Steve: And I did have - Scott Stone tweeted, he's @sstone68, he tweeted: Except my kids have an IR-controlled train set that sets off the smoke alarm's test mode. Not so brilliant. Huge fan of SN, keep it up. So, okay, it's not without its side effects, but still just extremely clever.

Leo: Very, very great.

Steve: And from the Twitterverse I've got three little quickies. @infoholic Steve Remington tweeted regarding SN-307. He said the Gmail plus label email tip, many sites incorrectly implement email validation and do not allow the "+" character in email addresses. And similarly @rulerot tweeted, his name is Andrew, he said, "I used to pad my Gmail address, too. But too many websites think that '+' is invalid. Others have taken it and then choked on the back end." So I wanted to share that caveat about the tip that we talked about last week of using the plus in order to create sort of an account plus a label for the purpose of creating unique email addresses. Because it's done so infrequently, it's very clear that many email systems don't handle it properly, which is way annoying.

And @JBTechSec, whose name is Jack Brennan, tweeted: "Just finished 'Zero Day.' Not a masterpiece, but very enjoyable. I finished it in two days. Thanks for the tip." Now, this is my segue to tell you about a book that I'm at 66 percent of, and I have been having so much fun on my Stair Climber with this book. When I was talking about "Zero Day," which of course our friend Mark Russinovich wrote, and recommended it, and I've had a ton of great feedback, some other people tweeted, "If you liked that, you're gonna love this." The book is "Daemon."

Leo: Oh, yeah. Oh, you're way behind.

Steve: Leo.

Leo: And there's a sequel to it, too. You're going to have to read that, too.

Steve: I know, and I am so glad because I don't want this to ever end.

Leo: I know, it's excellent.

Steve: Most books you sort of get into it, and it plateaus, especially Hamilton. It's like, how long more do I have of this? I mean, it's good, and you're enjoying it. But if I were to draw a curve I would say you kind of ramp up, and then you plateau. This darn book, it keeps getting better. I mean, it gets better and better. It's like, as I'm reading, it's like oh, my goodness. Oh, my god. I mean, this author does everything you dream he might do with this concept. Oh, my god, it is good. So it is a masterpiece.

Leo: Oh, yeah.

Steve: And I had to recommend it. So it's "Daemon," which of course is from the UNIX world, the name for processes that run in the background and just do work for you. I'm not going to spoil this for anybody. But no one who listens to this podcast could possibly read this and not just be blown away. It is fantastic.

Leo: It's Daniel Suarez. By the way, I met him about a year ago. Great guy, and this is his first novel. That's the amazing story about this. He created this - and by the way, here's a nice little autograph from Daniel I really cherish. He created this novel while he was working as a programmer. He obviously, as you read it, you know has a real understanding of computer technology. This is a very - just as Mark Russinovich does. It's an intelligent book.

Steve: Oh, it's just - it keeps getting better. It's like, oh, my god, how can this keep getting better?

Leo: And this is the sequel to it, FreedomTM. And you've got to get that, too, because it...

Steve: It's like a ramp. You just keep going up higher and higher. It's like, oh, my god.

Leo: How did we miss not telling you about this book? We all talked about it when it came out. We interviewed him. And actually he's going to come on our Triangulation show soon because he's been writing his new book, which is about predator drones. And he's going to come on and talk about that.

Steve: I'm reading it. I don't care, I'll read anything this guy ever writes. It is just...

Leo: Good, isn't he?

Steve: It's spectacular.

Leo: Good writer.

Steve: So, highest, highest recommendation. I'm late to the party, Leo. But anybody else who is, too, just hit pause and buy this thing.

Leo: Actually, you know, my 16-year-old son loved it, too. There's enough action in it, it really kept his attention. And the computer science in it is very well done.

Steve: Yes, and massively multiplayer gaming comes in, and Internet, and all the tech is correct. Oh, I'm stunned.

Leo: And you have to read the sequel because it ends in the middle.

Steve: Oh, believe me. I'm just - I'm so glad that this isn't ending at 66 percent because, like, knowing that there's another one of these, oh, goodness.

Leo: And it comes, by the way - we'll talk when you finish the second one. It has a great ending.

Steve: Oh, good.

Leo: You're going to love it.

Steve: A real quick short note from a SpinRite devotee, Harvey A. Russ. He wrote, "Okay, this was an emergency. My TiVo puked. The WeaKnees tech support page said that the problem with my TiVo looks like a disk failure, and that I had to give up. Well, I have the fix: SpinRite 6. Yes, I resurrected the pair of disks in my Series II TiVo using the handy-dandy trusty SpinRite. Steve, thank you for your knowledge in hard drives and technology in general. I've been using SpinRite since v1.0. Your faithful follower in technology, Harvey."

Leo: That's great. Not an easy thing to do because you have to pull it out of the TiVo and put it in a PC. But it works.

Steve: And if you've got all your shows on there, and you're otherwise SOL, as they say, SpinRite comes to the rescue.

Leo: Actually that's a second recommendation on there because WeaKnees is the place to go if you're a TiVo user. I love WeaKnees.com. They're very nice people.

Steve: Yeah, they are. And in fact they have a nice 48-bit Linux kernel that I was able to use for my old Series I TiVos in order to get them to get out of that 32-bit barrier.

Leo: Yes, two K's. Actually, both work. That's interesting. So one or two K's, depending on how you want to spell it.

Steve: Oh, interesting.

Leo: But two K's does work.

Steve: Good for them.

Leo: Yeah, they're smart. Because there's two ways to spell it, isn't there. Now, Steve Gibson, I have questions. And I presume you wouldn't have given me these questions if you didn't have answers.

Steve: Or sometimes they're just great tidbits. In fact, this first one is incredibly clever.

Leo: Good. It goes back to that read-only USB thing we've been talking about for a while. Marco Gouveia e Silva in Funchal, Madeira Islands, Portugal says: Hi, Steve and Leo. I've been a listener of Security Now! almost since the beginning, and I also listen to some other TWiT shows. Thank you. Love what you do. Hope you don't stop. My apologies for my Portuguese, Marco. I think I found a great way of making a USB thumb drive read-only, but I need your opinion and blessing, Steve. What if you used a CD file system on a USB stick? ISO9660, which is what CDs use, is read-only by design.

Steve: Yes. Very clever.

Leo: Interesting. He says: I'm a happy almost-only Linux user, and I've read this on a magazine called Linux Format. So here goes the way of doing this on Linux, but of course you could do it with Windows and Mac with the right software.

Use some CD-burning software, he says, K3b, Nero, so on, to create a CD ISO image containing the files you want to have on the key as read-only. You can also do this from the command line if you are a Linux fan with mkisofs (make ISO file system) -r -V discname -o somefiles.iso file1 file 2, et cetera. Discname of course is the volume ID that will be given and used when mounting the device. You can list as many files as you want on the command line, or of course you can use globbing or even specify a whole directory. But it's easier just to use some CD-burning software to do this.

Now you've got to burn the ISO - this is the tricky part. It's easy to make the ISO. You might even have an ISO if you downloaded a Linux distribution, for instance. Now you can burn the ISO to a USB stick. You start with the stick not mounted, so unmount it and then run dd, use dd if= the path to the file, to the ISO file. That's the if, the in file. The out file is the device, the USB device. So if you're a Linux user you'll know, it'll be in /dev/sd and some number. Block size 2K, I think that you could change. But anyway, you do have to use the base device, obviously, and not a root partition on it, not a mount partition. You want it to be unmounted. And it's going to erase the entire thumb drive. Dd is on Windows. If you Google search you can find it. But of course it's on Mac and Linux operating systems.

Wait for the drive's LED to stop flashing, that's important. Unplug and then plug it in again. Your OS will mount it as a read-only device. The files on this file system will be read-only. But here's the question for you, Steve: Is this good enough? Is this safe? Does it get the Gibson Seal of Approval? Thanks for the podcast. I've learned so much from it. Keep up the good work. Mark. What do you say?

Steve: I think it is incredibly clever. It's absolutely the case that the OS would present to any software running in the operating system a read-only device. So any standard file-writing calls would absolutely fail. If you tried to alter the contents, the OS would say this is not writable and fail the call. The only vulnerability is that obviously technically it's still a writable device. So someone could create, you could have theoretical software that would unmount it and access it in raw mode and then go out and alter the CD image in order to incorporate additional files. But no such thing exists.

So I just think this is really cool and clever. So because there's a theoretical way you could get around it, it's like, eh, you know, having a write-protect switch that you have verified on a USB stick is going to be safer. But doing both would give you lots of protection because then you would be safe even if, for example, you forgot to have the switch set the other direction. So I just - this was such a clever idea, I wanted to share it with our listeners as, like, this is thinking outside the box, and it's really a great solution. And, yes, the fact is it would stop all malware from installing itself.

Leo: So malware can't override these settings. It can't say, oh, ignore the read-only.

Steve: Correct, because the image itself is closed, and the file system has no provision for, like, dynamically relocating, marking files deleted and all that. None of that exists in that 9660 file system. It's just a way of providing a static fixed image, which is what makes it so cool, such a great solution.

Leo: Yeah. Question 2, Glenn Edward in Nottingham, Maryland. He wonders whether Adobe's Shockwave player is really necessary: Times are tight, as they say, and I can't keep adding RAM sticks to this old PC of mine, or afford a new one with a lot more RAM capacity. So I like to keep my PC's installed software to a useful minimum. And I keep seeing both Adobe Shockwave and Flash listed as things I must have. But I wonder if that's not just a load of Adobe baloney, and that Shockwave is just about as useful as having the RealPlayer plug-in installed. I've wondered this myself because everything uses Flash, but Shockwave is an old technology that I don't - it's rarely used anymore. I'm sure there's some business or

educational applications that need Shockwave, but how likely is it the average Internet user's going to run into it? So I'm hoping you'll tell me "not very," and I can eliminate the Shockwave plug-in and not keep it updated. Glenn Edward of Nottingham, Maryland.

Steve: Not very, and eliminate the Shockwave plug-in and not keep it updated. That's exactly right.

Leo: Yeah. And then if you need it, it will tell you.

Steve: Yes. If you need it, then you can decide if it's worth it. But that's exactly the same advice we have for any of our low-utilization things like RealMedia, although Elaine sometimes gives me a little poke and says, Steve, you realize I'm transcribing the podcast with a RealMedia player.

Leo: Really?

Steve: Yes, I think she has foot pedals or something.

Leo: She's so old-fashioned.

Steve: Well, no, I mean, it's like the only thing. She's really up-to-date with things, but it's the only thing that does what she needs. She can't find anything else otherwise. So and of course I don't think she's out surfing in strange dark corners of the Internet and downloading images...

Leo: Well, and Java, that's another example, we were talking about the Facebook plug-in, which does use Java, apparently only on the Mac. It looks like an EXE on Windows machines. But we've said before, don't have Java on there unless you need Java. Java 7's coming out tomorrow. And a lot of people might say, oh, quick, and go out and get it. No. If you don't need it, don't have it.

Steve: Yes. And so Shockwave was an earlier technology. Once upon a time there were a lot of games. Remember the bowling the elves or something?

Leo: Yeah, Elf Bowling?

Steve: Elf Bowling or whatever? Those sorts of things were done in Shockwave a decade ago.

Leo: And I'm told some gaming sites still have Shockwave.

Steve: But if you're not a person who knows you need it, get rid of it, absolutely. And as you said, Leo, if you go to a site that says, oh, you need to have Shockwave in order to see this postcard from your aunt or something, it's like, well, okay, Aunt, I know you love me, I'm not going to load Shockwave.

Leo: Yeah, you can decide.

Steve: I can live without it, yes.

Leo: Is it so horrendously buggy that it probably is not safe to...

Steve: It's, yeah, I mean, I would say it's probably worse than Flash because it's getting less attention. And anything with less attention has got gremlins squirreled away in it.

Leo: Incidentally, now, SDA1, who is apparently a USB key plugged into our chatroom, says that the Skype on the PC Facebook uses EXE loader, but it is for a JAR file, which of course is possible. So it may still need Java. I would expect it would. Why would they write an EXE file for Windows and use Java on the Mac? You might as well just write one in Java and put it everywhere.

Steve: Right.

Leo: So, yeah, you probably will need Java. There are a lot of reasons to have Java on there. Greg in Florida reminds us of a simple iPhone/iPad password improvement. He says: Steve, your recent comment about iPhone passwords reminded me of a great way to help secure an iOS device. I'm the only person I know that uses it. But if you turn off "simple passcode" in the settings, instead of the numerical keypad, which only is four digits or whatever, you get a full QWERTY keyboard to enter the password. Even if you still use a short code, the increased character set makes guessing much, much harder. It also makes shoulder surfing a bit more difficult, as well. So in other words, don't use that numeric keyboard which only gives you four digits. Use the full keyboard.

Steve: Yeah. And you know, a number of people had mentioned this before. I just kept forgetting to relay it. I wanted to make sure that our listeners knew that that option existed. You turn off "simple passcode," and then you've got the full keyboard, so you're not limited to four characters. You can do anything you want to there, if you really want to crank up the security on accessing your iPhone or iPad.

Leo: Awesome. I actually have the feature turned on that says, if somebody guesses 10 times incorrectly, it erases it. And I feel that's sufficient, as well.

Steve: Yes, because that means someone has commandeered your device.

Leo: You only get 10 shots, yeah.

Steve: Yes. And every time we dock, our device is backed up into our local machine, so we can replace it and reload it. Or if they say, oh, I'm sorry, I tried to play a game on your iPad while you were away, and it seems to have wiped it out, well, then, you just dock it and bring it back to the condition it was.

Leo: Yeah, not such a loss.

Steve: Yeah.

Leo: MyCloud will make that even better. Moving right along, Steve in Columbus, Ohio asking: Why is all personal data not encrypted on a company server? After reading all these security hacks in the news and almost being a victim in the MtGox breach, the Bitcoin exchange breach, one question keeps coming to mind: Why is it companies only feel the need to hash or encrypt passwords and financial data, if even that, and not also encrypt other data like email address, phone, et cetera? Even data as simple as my first and last name, you know, why not hash that? I understand that financial and passwords seem the most important, but shouldn't all my information be protected? Is there a technical limitation to hashing that much data? Is it laziness? I look forward to your response.

A quick note about my earlier "almost compromised" remark. About one minute after receiving the email about the MtGox hack I was simultaneously knocked out of my Gmail accounts (desktop, laptop, and Android) and was forced to change my password because of suspicious activity. I was not compromised because I had Google's two-step verification turned on, and for safety I immediately generated and inserted a new password with LastPass. Thanks for Security Now!.

Steve: And that, yeah, that reminds me that one of the advantages, we were talking about OAuth and the idea of using a secure site to authenticate yourself, well, if you use, for example, Google two-step verification, then you get that additional level of safety when you authenticate to the site that you're being referred to, so that's handy also. But as for Steve's question as to why all of our data is not being kept encrypted, it's just because they don't have to. There's...

Leo: It's not like a huge hardship to do it.

Steve: It is zero, Leo. It is the developers, the programmers caring to do so. And to the degree that these systems are purchased from a central location, from like a kit of some sort, it's just criminal that the kits haven't done this because then everybody else who used those kits or those turnkey solutions would automatically have everything encrypted. So this is another sign of it just being the early days still. Certainly at some point there will probably be legislation which requires the encryption. I don't know how else it's going to happen except that it's just you're forced to do it, and the penalty of ever having unencrypted data escape, which would demonstrate that you were in violation of the law, would then be very high.

But nothing prevents it. Encryption takes no time, no overhead. I mean, there's no excuse for not having our data encrypted. It does need to be encryption rather than hashing. We talk about hashing passwords because we never need to unhash them. In fact, the way we verify them is that we hash the original one and keep the result. Then we hash what the user gives us later when they want to come back and see if they match. But in the case of things like first name, last name, address and so forth, where we actually want to get that, well, then, there we need to encrypt that so that we can decrypt it later. But it absolutely should be stored in encrypted form so that when these database files are downloaded, all they get is pseudorandom noise, I mean, just nothing. Absolutely, just like LastPass does.

Leo: Moving along, this is from Lewis Barnett at WhosTheMuse.com. You've got to read it carefully, WhosTheMuse.com.

Steve: Who's the muse.

Leo: WhosTheMuse.com. I'm thinking security, so I'm going w host, then I'm stuck, he muse dotcom. As a geek who is already running a newer version of Windows, I really would like to know what do you plan to do after support for Windows XP expires, which is not instantly. I mean, we've got a few years. As I listen to Episode 306 of Security Now! I know there are still 1,020 days left. But have you given any thought as to what you'll do after that, Mr. Steve Gibson? I know you dislike adopting new technologies - boy, he really thinks you're really a curmudgeon - but will Windows 7 be advanced enough in three years for you? Plus, what was that Star Trek noise in the background? I love the show, and keep it up. I mentioned the Star Trek noise in the background.

Steve: Yes, you did. Now, that was Episode 306. I just checked my Win7 screen, not the one I'm in front of, but the one where Skype is running, and it's showing me, I've got to remember that there's a desktop widget which shows you on Windows 7 the length of time before Windows XP security updates expire. And it is now 1,006 days. So not surprisingly, 14 days fewer than two weeks ago when it was 1,020. So as you say, Leo, I've got almost three years, or two and a half, I guess, something like that, to go. And Lewis, that'll be fine. I have 7 running on a tablet. I have 7 running to my side. I was doing my Bitcoin mining on 7. So I'm not using it. It's around. I'm sort of getting the feel of it, and I'm so happy I will have been able to skip over the Vista nightmare. So, yeah, I think two and a half years more, Win7 ought to be ready for me by then. I think the timing will work just right.

Leo: I actually like Windows 7. I'm using it now, by the way.

Steve: Oh, and Star Trek noises, many people tweeted about where it was that I found those high-quality Star Trek sounds that had, like, the engine noise removed from the background and everything. And so I found them again, and just for the podcast I tweeted the URL because it's too long for me to say it verbally. So if anyone wants to find the link to this website where they purified and just beautiful Star Trek sounds from all the various variations of the Star Trek series, Next Generation and the original and what was the floating island one? Can't remember.

Leo: You're asking the wrong guy. I'm not a big Star Wars fan.

Steve: Deep Space Nine.

Leo: I'm just teasing.

Steve: Deep Space Nine.

Leo: Oh, yeah, Deep Space Nine. That was with the Ferengi.

Steve: That's right. Anyway...

Leo: By the way, all on Netflix, every one of them. Netflix streaming.

Steve: All the episodes, yes.

Leo: All the old episodes, including the original series, Enterprise, Deep Space Nine, they're all there.

Steve: Okay. So anyway, Twitter.com/SGgrc. That will show you my tweet timeline. And the last tweet there, I don't tweet that often, so you'll still not have to dig very far, is the URL to this site that's got really, really good Star Trek cleaned-up pure noises. And I think that was the communication termination noise, which I've got as my BlackBerry sound for incoming email. So it always does raise eyebrows when the phone does that. It's like, okay, Gibson.

Leo: [Making noises] No, those are Star Wars.

Steve: Yeah.

Leo: Luke - actually I'm going to read two together, so two questions in a row. And then your answer. Luke, aka Kellycarter on Thaurissan Guild "Cookies" - oh, it's Wow - an avid WoW player in Nashville, Tennessee and Azeroth - that's the realm in the World of Warcraft he plays on, apparently - wonders about Blizzard's newer authentication. Steve, I have to say I had a Gibsonian response the other day. I, as you might have guessed, love the game World of Warcraft. I loved how they used a football or an app to generate a code required to log in. I didn't know they were doing that, second factor authentication.

But recently, Blizzard, the company that makes Warcraft, changed how they do their security. They no longer require a code every time you log in, and they tell us they

are doing something on their end to validate that I am who I claim to be. But the thing that brought my alert level up is they're not telling us what it is they're using. We can't validate that they're doing the right thing or if they forgot something, or if it's only imaginary security. Is there any way you could check in on this for those of us that spend time in Azeroth? By the way, Steve, what class/race/spec would you like to play? For the horde. I'm sorry. You don't play World of Warcraft, do you.

Steve: Never.

Leo: You have a life.

Steve: I've never even seen it.

Leo: I played it for quite a bit, and then I realized I was losing my life. So now I play Tiny Tower on the iPad. So do you know what they're doing?

Steve: Well, let's go to number two, second question.

Leo: Oh, yeah, sorry. I warned you, but I didn't heed my warning. Scott Clark in Hamilton, Ontario, Canada also wonders and worries: I'm an avid fan of the work you do producing Security Now!. I'm a guild leader on the Skywall server of World of Warcraft and am acutely aware of the need for security to protect my account. I use a Blizzard Authenticator, which is a modified Vasco security token. Blizzard has long checked location data and locked accounts that were accessed from unexpected locations.

Recently without warning Blizzard implemented a change to their security policies. If they are confident in your identity when you log in, they're not going to require you to enter your Authenticator number, bypassing this measure entirely. Blizzard has not released details on how this identity check takes place, although presumably it's based on some mix of location, MAC address, and/or stored certificate.

There has been considerable debate on the forums as to whether this represents a weakening or a strengthening of our account security. Blizzard has not been forthcoming with details, and they do not provide an opt-out which would force use of the Authenticator. Personally I prefer the security of knowing that the Authenticator is required for all logins, versus the convenience of not entering the code each time. What I'd like to know is, by asking for the Authenticator code on each login, is this not strictly weaker than requiring it - you understood what I mean. Is it weaker not to ask for the code?

Steve: Okay, so here's what happened. Due to the insane popularity globally of World of Warcraft, years ago it became a real problem that users were using weak passwords, they were getting their World of Warcraft accounts hacked right and left...

Leo: Yeah, lots of cheating and stuff, too. I mean, this is a big problem.

Steve: Yeah, it's a huge problem. And people, as you no doubt, Leo, know, build up tremendous value in their identities, their online identities in World of Warcraft. So getting hacked, I mean, can be hugely expensive and traumatic for the game player because some bad guy gets in and, like, sells all your gold or transfers it somewhere else or does something, I'm not quite sure on the details. But I know that...

Leo: You said that as if you're a WoW player yourself.

Steve: Yeah, well, I did some research. So what happened was Blizzard decided they were going to come up to speed with multifactor authentication. And they added some years ago the Blizzard Authenticator, which is exactly identical to our wonderful little football that we've talked about for, like, logging into PayPal and eBay and so forth, where you press the button and you get the six digits and it's changing every 30 seconds and so on.

What then ensued was malware which would perform an effective man-in-the-middle attack - it was called emucor or emcor.dll - which World of Warcraft players were getting themselves infected with. So because Blizzard was requiring authentication every time, every time you logged in this emcor.dll would intercept in real-time your username and password and current display from your Authenticator and instantly ship it off to somewhere bad, where it would be immediately used to authenticate. You would be given the news that there was a problem with your authentication, while the other person was in real-time logging into your World of Warcraft account and emptying it, selling off your gold and jewels and who knows what mischief they were getting up to.

So what happened was Blizzard developed a hybrid approach. They backed off of requiring the Authenticator every time, only needing it in instances where they suspect you may not be where they have some reason to believe you have been using WoW from before. There are, as our writers here and podcast listeners suggest, there are a number of ways that World of Warcraft, the Blizzard people could know where you are. You're using the same IP address that you have used for the last five weeks.

Leo: I wish they'd tell us because then we could judge it. But let's say they do it kind of as LastPass does it, where the first time you log in you need the Authenticator. Once you do that, they put a certificate on your system, and then they check for the certificate. That would be pretty good.

Steve: Yes. The problem is you could - the certificate could get lifted, too. I mean, first of all, if something's bad in your system, it's pretty much game over. If you've got anything high value on your system while you've got malware present, then you're in trouble. So the cert is one thing. They could also, for example, read the MAC address from your adapter, as was suggested. They don't receive the MAC address over your connection. They get your IP address over your connection, but they could read the MAC address from your adapter, which is globally unique, although subject to change. Or just store a cookie of some sort on your system. I mean, anything that they do to say this looks like a machine that we have reason to believe, I mean, there's all kinds of ways to associate with a machine.

Leo: Apparently, if you change IP address, that is sufficient to trigger reauthentication.

Steve: I would use IP address as the first thing that I looked at. But all hard drives have serial numbers. So you can get the serial number off the hard drive.

Leo: Well, and we know with, what was that super cookie thing, we know there's ways to identify almost uniquely, in fact, if not a hundred percent uniquely, any computer.

Steve: Right.

Leo: With stuff you can easily get over the Internet.

Steve: So I think the hybrid approach makes more sense if you're going to have a high incidence of malware which is compromising your authentication by performing a man-in-the-middle attack, which is in fact what happened.

Leo: All right. So in other words - I think, you know, they've got to balance this with a lot of normal users who don't want to get a security token, but who also may want to use...

Steve: Actually it's required. It's required, Leo. They were selling it at cost. It was $6. And if you were going to continue using World of Warcraft, you had to get one. The problem was that bad.

Leo: Shows you how long it's been since I've logged on because I didn't know that.

Steve: And so I do think, though, that...

Leo: That would have stopped me, by the way, right there. I would have said, aw, screw it, I'll do some other game.

Steve: The upside to using a multi-vector authentication is that then you're not requiring someone to use the Authenticator every single time, every single time they log on. Many users appreciated it because they felt the danger within the community. But the fact is, locking onto your IP address is going to be pretty good. That would require a much more sophisticated attack using your machine as a proxy in order to loop through and have the bad guys do something remotely. So that would be not like - you could write that, but so far it doesn't seem to exist.

Leo: Our last question, I'm sorry to say. Patrick, an old soul in Laramie, Wyoming brings us our Wrap-Up Philosophical Discussion Topic of the Week: Are we losing the forest, he asks, for the trees? Steve and Leo, last week's topic about the growing importance and role of identity over the Internet made me wonder, which is a good thing, are we losing the forest for the trees? Maybe I'm different than the generations coming after me, but I prefer to hang out with my friends face to face, rather than a video chatroom. I prefer to go to the bank and talk to the tellers - well, good luck doing that, I doubt you'll be doing that much longer - rather than go online, although I do that, as well. I prefer to sit - this guy's sounding like an old fart, now. I prefer to sit in front of a slide projector - do they still make those? - with my family than to flip through someone's Facebook album. While I realize that the Internet is very powerful, and it enables things that we would never have imagined a decade ago, I just have to wonder if it's really such a good idea to move everything to the Internet, which is the direction it seems we're headed. Coming from the perspective of a kid growing up with computers and technology, I feel like perhaps we all need to take a step back and really ask ourselves, is this really the best direction to head in? Am I just starting to sound like my grandpa, or is there any legitimacy to what I'm saying? I'm curious to hear your thoughts. Thanks for everything you do. Look forward to many years to come. Patrick.

Steve: Well, Leo, I love texting. I just - I love my phone, and I've got a network of friends that I'm in constant contact with. And Twitter has been a boon for, really, for connecting me to our Security Now! listenership in a way that I hadn't been before, so that I don't miss things going on; and I'm able to deliver, I think, a better podcast every week as a consequence of it. And of course Wikipedia, I mean, and the 'Net itself. As an information worker, I am hugely empowered by this.

And I was just hearing some conversation, some dialogue the other day, maybe it was on a TWiT show, talking about how - oh, it was on the radio this morning, how Facebook has really revolutionized relationships. They were enumerating the regrets people have, like the top five regrets people have in their life. And one of them was that they had lost contact with their friends. And the people, the two DJs were bantering back and forth. And they said, you know, I'm, like, I've reconnected with all these friends that I had lost touch with, thanks to Facebook, which I think is many people's experience. So certainly there's a depersonalization going on. But boy, I think on balance it's just a boon. It's communication.

Leo: Yeah. But there is an interesting backlash going on among even young people, whom I gather Patrick is since he said he grew up with computers. In fact, we had this discussion, I can't remember what show it was on, that bookstores - and maybe it was This Week in Google, which is coming up next - that bookstores aren't going to go away, they're just going to change because we do need some way of getting together in real life, in person, face to face.

But, see, you and I are a rare case. We prefer to stay at home and do our computer thing. We're introverts. And but we're a minority. I think most people do prefer to get together. Oh, Patrick's in our chatroom. He says he's 21. So he's a kid, even though he sounds like an old guy. I think in fact my daughter's been saying this. She's 19, and she's been saying this for some time.

Steve: Wait, saying what?

Leo: She says, in my generation there is a move away from the Internet.

Steve: Wow.

Leo: And it's of course probably a pendulum. But she says that she believes, and she's I think one of them, that face to face is better. And there is a move afoot among these younger people in that direction.

Steve: I wonder, though, if that's a move back from absolute over-insanity saturation.

Leo: Well, that's what I mean by a pendulum. I think it swings.

Steve: Well, but, I mean, like there was a tendency maybe to get completely on the 'Net in a way that even you and I haven't yet, where it was like obsessive Internet use. And so for Abby, she's backing away to, like, a more...

Leo: What you and I would consider normal.

Steve: Exactly, more even keel sort of usage.

Leo: Well, and then there's Jaron Lanier, who of course was a pioneer in virtual reality, who now eschews all things technological. There was just an article about him in I want to say The New York Times. And he's written a book saying "You Are Not a Gadget." And he's really lobbying hard for turning our backs on technology in at least some respects. And don't forget Cliff Stoll, who was an astronomer, computer scientist, wrote a great book about hacking, who has also become an anti-technologist. So I don't know, I mean, we see Tweetups now, as HishMaj is pointing out in the chatroom, where people who know each other from Twitter meet specifically so that there's some face to face.

Steve: Yeah, and in fact I have amazing relationships with people in GRC's newsgroups whom I've never met, probably never will. But I'm sort of curious about them, and I've wondered, boy, you know, if I were to host a big gathering, what would that be like? That would be weird, to take us out of our virtual realm.

Leo: I'll tell you, I think this is why there's something deeply satisfying about South by Southwest and other conferences like that. When I went to Foo Camp with 300 other people, when you meet somebody that you only know on Twitter, you know their handle, there's something deeply satisfying about saying, "Hello, hey, you're @," you know, and saying, "Oh, Mickey. Oh, it's nice to meet you." And so I think there's a certain value to that. And I just think that some of us have gotten so digitized that we forgot.

Steve: So digitized. So it's not replacing the real world. It's just supplementing.

Leo: And I'm with you, I mean, the value is huge.

Steve: Oh, goodness, yes.

Leo: And you're kind of a late convert, frankly. I had to talk you into Twitter.

Steve: Yeah. I just passed, just two days ago, 22,000. Or was it, no, it was yesterday, 22,000 followers.

Leo: That's great.

Steve: So I'm enjoying it. And it's super useful for me. So thank you, everybody, for sending your thoughts over...

Leo: Oh, that's funny, I met Patrick. He was here last week for the Security Now! episode, he's telling me. Oh yeah, I remember you, Patrick. That's very funny.

Steve Gibson is on the Twitter as @SGgrc. GRC stands for Gibson Research Corporation. That's his website, GRC.com. So this all makes sense if you start to understand that. @SGgrc is his Twitter handle. GRC.com is the place to go if you'd like to know more about all the things he talks about. Of course all the shows are there, 16KB versions, transcriptions so you can read along as Steve talks. It's all there at GRC.com.

And don't forget, of course, SpinRite, the world's finest hard drive maintenance and recovery utility. It's a must-have. If you have a hard drive, you have to have SpinRite. We do this show every Wednesday, 11:00 a.m. Pacific, 2:00 p.m. Eastern, 1800 UTC at live.twit.tv. We do invite you to join us then. There's a party. Can you hear the party going on in the other room?

Steve: Yeah, I heard something.

Leo: I guess we're having a - I guess they are meeting face to face now. The kids today. And they just love it. You know what the problem is, we have too many darn people. We have 18 people jammed in that little room next door. So everybody needs to run out and buy a brick right now so that we can move to the new TWiT Brick House. Steve, we've got two more Security Now! episodes from here, and then we'll be in the new facility.

Steve: No kidding.

Leo: July 24th is our move date. And I know you're coming up for the party August 21st. I look forward to that.

Steve: Yup.

Leo: If you haven't yet bought a brick, bricks.twit.tv. It helps us build the studio, but it also puts you on the Wall of Honor right there in the entryway. It's just - it's shaping up so cool. It's really, really fun. Thanks everybody for being here. Steve, we'll see you soon at GRC.com and next Wednesday for Security Now!.

Steve: Thanks, Leo.

Leo: Take care.